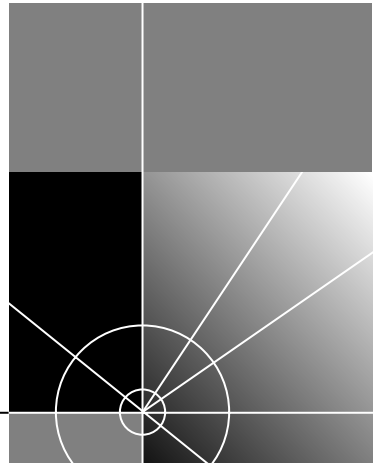
SuperStack® II Switch 3900 and Switch 9300 Administration Guide

Release 1.0.0



http://www.3com.com/

Part No. 10005623
Published April 1998

3Com Corporation
5400 Bayfront Plaza
Santa Clara, California
95052-8145

CONTENTS

PART IV BRIDGING PARAMETERS

8 ADMINISTERING THE BRIDGE

9 ADMINISTERING BRIDGE PORTS

About This Guide

This *Administration Guide* provides all the information that you need to configure and manage your SuperStack® II Switch 3900 or Switch 9300 after you install it and attach the system to your network. Before you use this guide, you should have already installed and set up your system using the *SuperStack II Switch 3900 Getting Started Guide* or the *SuperStack II Switch 9300 Getting Started Guide*.

This guide is intended for the system or network administrator who is responsible for configuring, using, and managing the system. The guide assumes a working knowledge of local area network (LAN) operations and a familiarity with communications protocols that are used on interconnected LANs.

If the information in the Release Notes that are shipped with this product differs from the information in this guide, follow the Release Notes.

Most user guides and release notes are available in Adobe Acrobat Reader Portable Document Format (PDF) or HTML on the 3Com World Wide Web site:

http://www.3com.com/

Finding Specific Information in This Guide

This guide is organized by the types of tasks that you may need to perform on the SuperStack II Switch 3900 or Switch 9300. The parts of the guide are described in Table 1.

Table 1 Description of Guide Parts

Refer to this part	To
I: Getting Started	Learn about SuperStack® II system administration
	Learn about the various system configurations and the quick commands to perform them
	Learn about password access to the Console
	Learn about the Administration Console menu structure and how to maneuver within the Console by using commands and moving between menus
	Set interface parameters (screen height and control keys)
	Run scripts of Console tasks
	Get help
II: System-Level Functions	Set up the system for management access through serial ports or using IP and setting up SNMP
	Administer the IP management interface
	Configure SNMP community strings
	Set up trap reporting
	Configure system parameters, such as name, date/time, and passwords
	Baseline statistics
	Save, restore, and reset nonvolatile data
III: Ethernet Parameters	Display statistics for and label Ethernet ports
	Set the autonegotiation feature
	Set port mode options
	Set flow control options
IV: Bridging Parameters	Configure bridge and bridge port parameters
	Administer the parameters for bridges and bridge ports under the Spanning Tree Protocol
	Display and configure bridge port addresses
	Display and configure trunks
	Display and configure virtual LANs (VLANs)
V: IP (Internet Protocol)	Configure IP interfaces and IP protocol parameters
VI: Appendix	Get technical support
	Return products for repair
Index	Quickly locate information on tasks and topics

Conventions

Table 2 and Table 3 list conventions that are used throughout this guide.

Table 2 Notice Icons

Icon	Type	Description
	Information Note	Information that describes important features or instructions
	Caution	Information that alerts you to potential loss of data or potential damage to an applications, system, or device
	Warning	Information that alerts you to potential personal injury. Follow all instructions carefully.

Table 3 Text Conventions

Convention	Description
`Screen displays`	This typeface represents information as it appears on the screen.
`Syntax`	The word "syntax" means that you must evaluate the syntax provided and then supply the appropriate values for the placeholders. Example: To set the date, use the following syntax: `mm/DD/yy hh:mm:ss: xm`
`Commands`	The word "command" means that you must enter the command exactly as shown and then press Return or Enter. Commands appear in bold. Example: To update the system software, enter the following command: **`system softwareUpdate`**  *This guide always gives the full form of a command in uppercase and lowercase letters. However, you can abbreviate commands by entering only the uppercase letters and the appropriate value. Commands are not case sensitive.*
The words "enter" and "type"	When you see the word "enter" in this guide, you must type something and then press Return or Enter. Do not press Return or Enter when an instruction simply says "type."
Key combinations	If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press Ctrl+Alt+Del.

(continued)

Table 3 Text Conventions (continued)

Convention	Description
Words in *italics*	Italics are used to: ■ Emphasize a point. ■ Denote a new term at the place where it is defined in the text. ■ Identify menu names, menu commands, and software button names. Examples: From the *File* menu, select *Print*. Click *OK*.

Documentation for the SuperStack II Switch 3900 and Switch 9300

The following documents comprise the SuperStack II Switch 3900 and Switch 9300 documentation sets. Documents are shipped with your system in one of two forms:

- Paper documents that are shipped with your system or with optional components. They are listed in the next section.
- SuperStack II 3900 and 9300 Documentation CD with online versions of the paper documents. See "Documents on CD-ROM" on page 5 for more details.

Paper Documents

These documents are shipped with the SuperStack II Switch 3900 system and the Switch 9300 system:

- *SuperStack II Switch 3900 and 9300 Unpacking Instructions*

  How to unpack your Switch 3900 system. Also, an inventory list of items that are shipped with your system.

- *SuperStack II Switch 3900 and 9300 Release Notes*

  All of the new features, system issues, known problems, and software corrections for the software release. It also describes any changes to the Switch 3900 system's documentation.

- *SuperStack II Switch 3900 and 9300 Quick Installation Guide*

  How to perform a quick installation of your system. For more details on installation, see the *SuperStack II Switch 3900 Getting Started Guide* or *Switch 9300 Getting Started Guide.*

- *SuperStack II Switch 3900 Getting Started Guide* or *SuperStack II Switch 3900 Getting Started Guide*

  All the procedures necessary for getting your system up and running, including information on installing, cabling, powering up, configuring, and troubleshooting the system.

- *SuperStack II Switch 3900 and 9300 Command Quick Reference Card*

  All of the Administration Console switching commands for the Switch 3900 and Switch 9300.

These documents are shipped with optional devices:

- *1000BASE-SX/1000BASE-LX Gigabit Ethernet Module Installation Guide*

  How to install the optional Gigabit Ethernet module.

- *SuperStack II Switch Advanced RPS User Guide*

  How to install the Advanced Redundant Power Supply (RPS) and how to use it to provide redundant and resilient power supplies for the Switch 3900 and Switch 9300.

- *SuperStack II Switch Advanced RPS Y Cable Type 2 User Guide*

  How to install the Y cable with the Advanced Redundant Power Supply (RPS) to provide fully redundant capabilities.

Documents on CD-ROM

The documentation compact disc that comes with your system contains these documents:

- Online versions of the paper documents that are shipped with your system and its components
- *SuperStack II Switch 3900 and 9300 Administration Guide* (this book)

  How to use the Administration Console and the management tasks that you can perform using it.

To order paper copies of documents that you see on the compact disc or to order additional compact discs, contact your sales representative.

Related Publications

Depending on how you install and manage your system, several related documents can provide helpful information:

- SNMP network manager documents

  The Switch 3900 uses SNMP (Simple Network Management Protocol), which can be accessed by a remote network management application. 3Com has network management applications for a variety of platforms. Contact your supplier for current product information. Each network management application includes a guide that explains how to manage your system.

If you are using network management software from another vendor, see the sections of the product's documentation that describe how to manage SNMP devices.

- SNMP documents

  3Com recommends these books for easy-to-read descriptions of SNMP:

  - Marshall T. Rose. *The Simple Book: An Introduction to Networking Management*. Englewood Cliffs, NJ: Prentice-Hall; 1996.
  - "Introduction to SNMP" Self-Study Guide. Order from 3Com: Part Number 3CS-350A.

- Telnet documents

  To manage the Switch 3900 system over a TCP/IP network using telnet, see the documentation that is supplied with your telnet application.

Documentation Comments

Your suggestions are very important to us. They help us to make our documentation more useful to you.

Please send e-mail comments about this guide to:

sdtechpubs_comments@3Com.com

Please include the following information when commenting:

- Document title
- Document part number (found on front or back page of document)
- Page number (if appropriate)

Example:

SuperStack II Switch 3900 and Switch 9300 Administration Guide

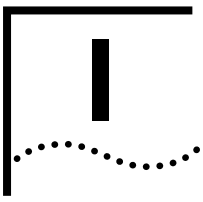
Part Number 10005623

Page 2-5 (chapter 2, page 5)

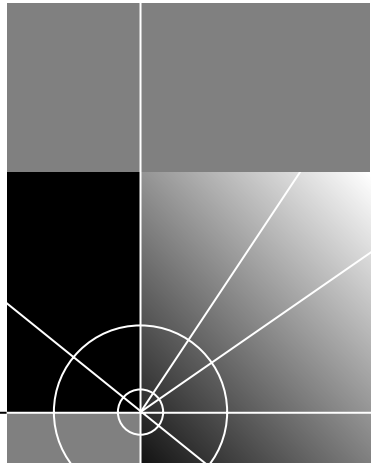
Year 2000 Compliance

For information on Year 2000 compliance and 3Com products, visit the 3Com Year 2000 Web page:

http://www.3com.com/products/yr2000.html



GETTING STARTED



1 ADMINISTRATION OVERVIEW

This chapter introduces you to system administration for the SuperStack® II Switch 3900 and Switch 9300 systems and briefly describes the system parameters that you can configure.

This chapter covers the following topics:

- About System Administration
- Configuration Tasks

About System Administration

The software is installed at the factory in flash memory on the system. Because this software boots automatically from flash memory when you power on your system, the system is immediately ready for use in your network.

However, you may need to configure certain parameters before the system can operate effectively in your networking environment. You may also want to view important MAC, port, bridge, VLAN, and IP statistics when managing your system. This book describes how.

The Administration Console software allows you to configure your system parameters and display statistics and counters. For more complete network management, use an external network management application.

Configuration Tasks

To help you perform a variety of configuration tasks, the system software provides the types of commands listed in Table 1-1.

Table 1-1 Types of Commands Associated with Configuration Tasks

Type of Command	Menus	Tasks
General system commands (Chapter 2, Chapter 3, Chapter 4, Chapter 5, Chapter 6)	**system**	Set system parameters, handle NV data, reboot
	log	Set severity levels and services for event logging
	script	Run scripts
	logout	Exit the Administration Console
Management setup commands (Chapter 3)	**management**	Set up the out-of-band management interface
	snmp	Set up the system for SNMP
Ethernet commands (Chapter 7)	**ethernet**	Manage Ethernet ports
Bridging commands (Chapter 8, Chapter 9, Chapter 10)	**bridge**	Set bridge parameters for the entire system, including Spanning Tree Protocol (STP) parameters
		Manage trunking of bridge ports
		Set bridge parameters for specific bridge ports
		Manage virtual LANs (VLANs)
Commands for administering IP (Chapter 11)	**ip**	Set up IP interfaces

The Administration Console commands are:

- Summarized on the *Command Quick Reference* card that is shipped with your system
- Listed completely in Chapter 2
- Described in detail in the rest of the book

2 How to Use the Administration Console

This chapter familiarizes you with these aspects of the SuperStack® II Switch 3900 and Switch 9300 Administration Console:

- Initial User Access
- Levels of User Access
- Using Menus to Perform Tasks
- Administration Console Interface Parameters
- Administration Console Remote Access Parameters
- Running Scripts of Administration Console Tasks
- Logging Out of the Administration Console

Initial User Access

The first time that you access the Administration Console, access the system at the *administer* level and press Return or Enter at the password prompt. The initial password is null. Subsequent access is described next.

Levels of User Access

The Administration Console supports three password levels, allowing for a range of SuperStack II users, as described in Table 2-1.

Table 2-1 Password Access Levels

Access Level	For users who need to	Allows users to
administer	Perform system setup and management tasks (usually, a single network administrator)	Perform system-level administration (such as setting passwords, loading new software, and so on)
write	Perform active network management	Configure network parameters (such as setting the aging time for a bridge)
read	Only view system parameters	Access only "display" menu items: **`display, summary, detail`**

Each time that you access the Administration Console, the system prompts you for an access level and password, as shown here:

```
Select access level (read, write, administer):
Password:
```

See "Setting Passwords" on page 4-5 for information about how to set passwords. The passwords are stored in nonvolatile (NV) memory. The following examples show how the menu structure changes based on your level of access.

Administer Access Example

When you enter the Administration Console with *administer* access, each menu contains all options. Here is the `system` menu for users with *administer* access:

```
Menu options:
------------------------------------------------------------------------------
  display                - Display the system configuration
  snapshot               - Display all configuration and status information
  softwareUpdate         - Load a new revision of system software
  baseline               - Administer a statistics baseline
  serialPort             - Administer the serial port
  consoleTimeout         - Administer console inactivity timeout
  password               - Set the console passwords
  name                   - Set the system name
  time                   - Set the date and time
  screenHeight           - Set the console screen height
  ctlKeys                - Enable/Disable Ctl-X (reboot)
  nvData                 - Save, restore, or reset nonvolatile data
  clearDiagBlock         - Clear the diagnostics block
  reboot                 - Reboot the system

Type 'q' to return to the previous menu or ? for help.
------------------------------------------------------------------------------
Select a menu option (system):
```

Write Access Example

When you enter the Administration Console with *write* access, the `system` menu contains a subset of the complete menu, focusing on the network, as shown here:

```
Menu options:
------------------------------------------------------------------------
  display           - Display the system configuration
  snapshot          - Display all configuration and status information
  baseline          - Administer a statistics baseline
  serialPort        - Administer the serial port
  consoleTimeout    - Administer console inactivity timeout
  name              - Set the system name
  screenHeight      - Set the console screen height

Type ‘q’ to return to the previous menu or ? for help.
------------------------------------------------------------------------
Select a menu option (system):
```

Read Access Example When you enter the Administration Console with *read* access, the **system** menu contains only the display options, shown here:

Only the display option in the baseline menu is available

```
Menu options:
------------------------------------------------------------------------
  display           - Display the system configuration
  snapshot          - Display all configuration and status informatio
  baseline          - Administer a statistics baseline

Type ‘q’ to return to the previous menu or ? for help.
------------------------------------------------------------------------
Select a menu option (system):
```

Using Menus to Perform Tasks

When you access the Administration Console, the top-level menu appears. To manage and monitor your system, select options from this menu and from others below it. Each menu option is accompanied by a brief description. Here is the `top-level` menu:

Option Descriptions

Menu options vary with the system configuration and your level of access

```
Menu options:
------------------------------------------------------------------------
  system                  - Administer system-level functions
  management (9300 only)  - Administer system management interface
  ethernet                - Administer Ethernet ports
  bridge                  - Administer bridging/VLANs
  ip                      - Administer IP
  snmp                    - Administer SNMP
  script                  - Run a script of console commands
  logout                  - Logout of the Administration Console

Type ? for help.
------------------------------------------------------------------------
Select a menu option:
```

The following sections show the menu paths for performing tasks from the top-level menu and provide a brief description of each top-level menu option. See "Selecting Menu Options" on page 2-8 for instructions on how to use the menu system.

The following menus display the options that are available for users with administer access. This access provides the most complete set of options.

system Menu

From the `system` menu, you can view the system configuration, set up your system for management, configure Administration Console interface parameters, work with nonvolatile data, and reboot the system. See Figure 2-1. For example, to restore nonvolatile data from the Administration Console, enter **`system`** at the top-level menu, **`nvData`** at the `system` menu, and then **`restore`** at the `nvData` menu.

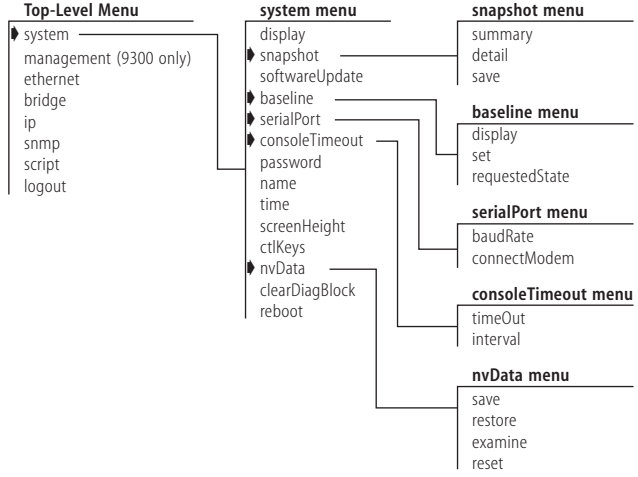


Figure 2-1 system Menu Hierarchy for Administer Access

management Menu (Switch 9300 only)

From the `management` menu, you can view summary and detailed information about the management interface (the 10BASE-T out-of-band management port that is located on the front panel of the Switch 9300). See Figure 2-2. For example, to view all summary information, enter **`management`** at the top-level menu and then **`summary`** at the `ethernet` menu.

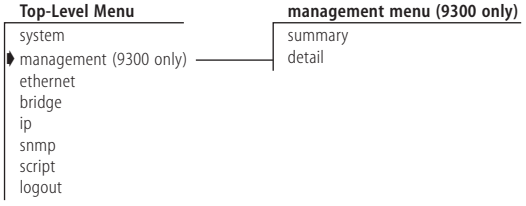


Figure 2-2 management Menu Hierarchy for Administer Access

ethernet Menu

From the `ethernet` menu, you can view information about and manage Ethernet and fast Ethernet ports. See Figure 2-3. For example, to view all Ethernet port statistics, enter **`ethernet`** at the top-level menu, and then **`detail`** at the `ethernet` menu.

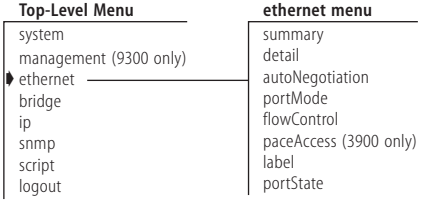


Figure 2-3 ethernet Menu Hierarchy for Administer Access

bridge Menu

From the `bridge` menu, you can view information about and configure bridge-level parameters, including those for the Spanning Tree Protocol (STP). You can also configure the bridge at the port level and administer virtual LANs (VLANs) and trunks. See Figure 2-4. For example, to set the Spanning Tree state for a bridge port, enter **`bridge`** at the top-level menu, **`port`** at the `bridge` menu, and then **`stpState`** at the `port` menu.

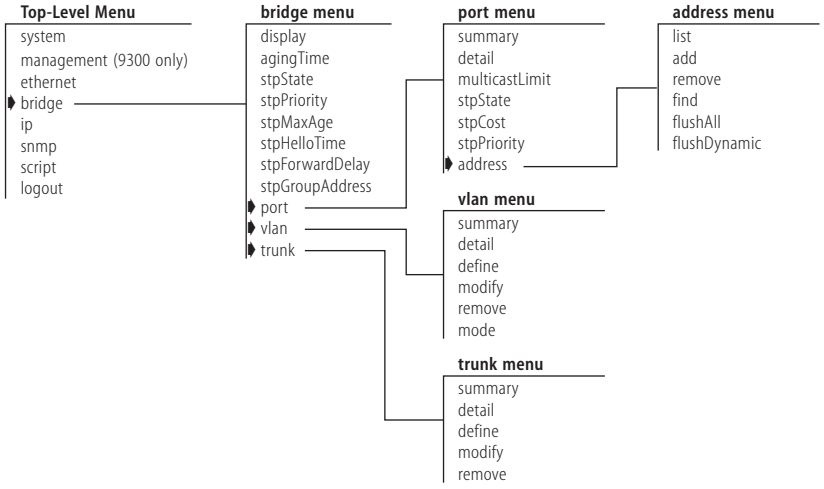


Figure 2-4 bridge Menu Hierarchy for Administer Access

ip Menu

From the `ip` menu, you can view information about and configure Internet Protocol (IP) interfaces and routes; administer the Address Resolution Protocol (ARP) and Routing Information Protocol (RIP); use the traceRoute feature; and ping IP stations. See Figure 2-5. For example, to define a new IP interface, enter **`ip`** at the top-level menu, **`interface`** at the `ip` menu, and then **`define`** at the `interface` menu.

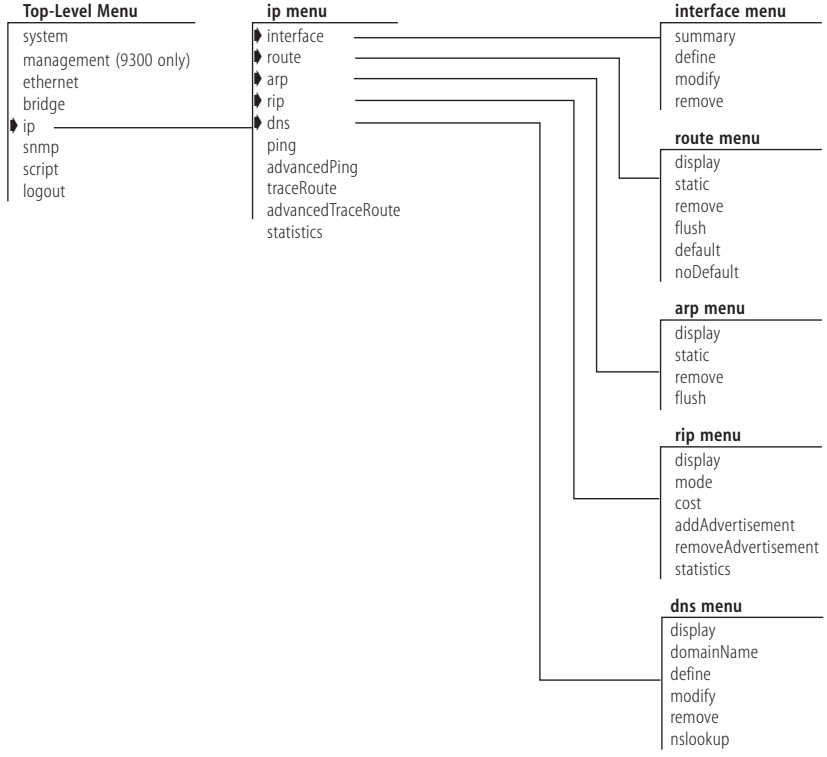


Figure 2-5 ip Menu Hierarchy for Administer Access

snmp Menu

From the `snmp` menu, you can configure the SNMP agent mode, community strings, and trap reporting. See Figure 2-6. For example, to flush all trap reporting destinations, enter **`snmp`** at the top-level menu, **`trap`** at the `snmp` menu, and then **`flush`** at the `trap` menu.

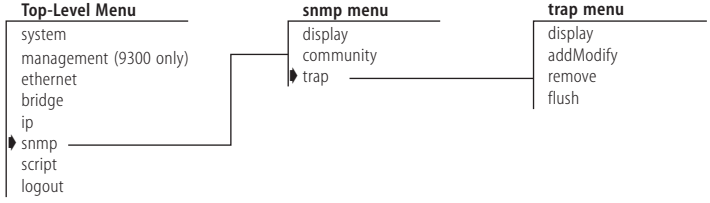


Figure 2-6 snmp Menu Hierarchy for Administer Access

Selecting Menu Options

To select a menu option at the selection prompt, enter its name (or enough of the name to uniquely identify it within the particular menu). For example, to access the `system` menu from the top-level menu, enter:

```
Select a menu option: system
```

or

```
Select a menu option: sy
```

Commands are not case sensitive.

When you enter a menu option, you either go to the next menu in the hierarchy or you see information for the option that you entered. The information is either a prompt or a screen display. If you enter the menu option incorrectly, you receive a prompt that what you entered was not valid or was ambiguous. Reenter the command from the point at which it became incorrect or expand a truncated command until it becomes unambiguous.

When a new menu appears, the selection prompt (with its choices in parentheses) changes to reflect your progression through the menus. For example, if you enter **`system`** at the top-level menu and then **`baseline`** at the `system` menu, the prompt changes at the next level:

```
Select a menu option (system/baseline):
```

Entering a command string

When you are familiar with the menu structure, you can enter a string of menu options at the selection prompt to go immediately to a task. For example, the command string for setting a baseline from the top-level menu looks like this:

```
Select a menu option: system baseline set
```

The most abbreviated version of the same command string is:

```
Select a menu option: sy b s
```

When you enter a command string, you move to the last menu level or option in the command string, and information relevant to that command appears. It can be a menu, a prompt, or a display.

If you enter a command incorrectly, the system displays a prompt telling you that what you entered was not valid or was ambiguous. Reenter the command from the point at which it became incorrect, or expand a truncated command until it becomes unambiguous.

Entering Values

When you reach the level at which you perform a specific task, the system prompts you for a value. The prompt usually shows all valid values (if applicable) and sometimes a suggested default value. The default may be the system default or the current user-defined value of that parameter.

The system displays the valid values in parentheses. The default value is in brackets. In this example, (`disabled, enabled`) are valid values. [`enabled`], shown in brackets, is the default:

```
Enter a new value (disabled,enabled) [enabled]:
```

Entering values in command strings

A command string can also contain the value of a command parameter. If you enter a value at the end of a command string, the task is completed, and the previous menu appear on the screen. For example, to disable a baseline from the top-level menu, enter:

```
Select a menu option: system baseline requestedState disabled
```

Using the Quit Option

To return to the menu that is one step higher in the hierarchy or to cancel an operation currently in progress, enter **`q`**, followed by Return or Enter.

To quickly move to the top-level menu without backtracking through intermediate menus, press the Escape key. The top-level menu appears on the screen. See "Logging Out of the Administration Console" on page 2-14 for more about leaving the Administration Console.

Administration Console Interface Parameters

You can change three Administration Console interface parameters: the screen height, functioning of the reboot control key, and the ability to modify system configurations from the Console.

Adjusting the Screen Height

You can change the Administration Console's screen height to increase or decrease the number of lines that are displayed on the screen.

The screen height setting does not affect the way that the system displays menus themselves. Rather, it controls the way that the system displays statistical summaries and other information that results from your use of the menus.

Each time that the screen output reaches the designated screen height, the system prompts you to press a key to display more information. You can set the screen height to infinite *(0)* if you do not want the system to display this prompt. At *0,* however, the screen output can scroll beyond the screen, depending on your screen size.

Default The default screen height is *24* lines. Most terminal screens have a height of 24 lines.

Top-Level Menu

- system
  - management (9300 only)
  - ethernet
  - bridge
  - ip
  - snmp
  - script
  - logout
- display
- snapshot
- ip
- softwareUpdate
- baseline
- serialPort
- consoleTimeout
- password
- name
- time
- screenHeight
- ctlKeys
- nvData
- clearDiagBlock
- reboot

1. To set the screen height, from the top level of the Administration Console, enter:

   ```
   system screenHeight
   ```

2. Enter the screen height in lines. Valid values are *20* through *200*, or *0* to receive no prompts.

   Example:

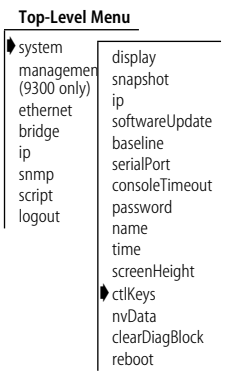
   ```
   Enter new screen height or 0 for infinite height [24]: 60
   ```

   The system prompts you about whether you want to set this value as the default.

3. Enter **y** (yes) to use this screen height as the default for future Administration Console sessions. Enter **n** (no) if you want this screen height to be in effect only for this session.

Disabling the Reboot Key

The Administration Console allows you to use the Ctrl+X key combination to reboot the system. You can change the setting to disable this feature.



1 To enable or disable the reboot control key, from the top level of the Administration Console, enter:

```
system ctlKeys
```

The system prompts you to enable or disable the functionality:

```
Enter new value (disabled,enabled) [enabled]:
```

2 Enter **`enabled`** or **`disabled`** at the prompt.

Administration Console Remote Access Parameters

You can reach the Administration Console remotely through a telnet session.

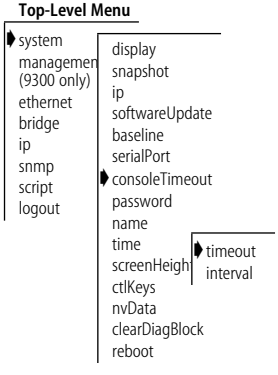
The Administration Console supports one telnet session as well as a serial connection.

You can enable the system to end remote sessions after a specified time period and specify the time interval before remote sessions end.

Enabling Timeout of Remote Sessions

You can configure the system to disconnect remote sessions after a specified time interval of no activity.

Default The default telnet timeout value is *disabled*.



1 To enable or disable the telnet timeout, from the top level of the Administration Console, enter:

```
system consoleTimeout timeOut
```

2 Enter the telnet timeout state (**`disabled`** or **`enabled`**).

The default timeout interval is *30* minutes. To change this value, follow the instructions in the next section.

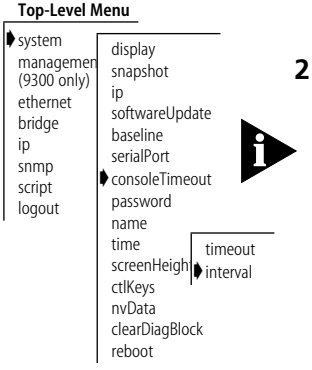
Setting the Timeout Interval for Remote Sessions

You can set the telnet timeout interval for remote sessions to any value from *1* minute to *60* minutes.

Default The default timeout interval is *30* minutes.

1 To set the telnet timeout interval, from the top level of the Administration Console, enter:

```
system consoleTimeout interval
```



2 Enter the telnet timeout interval: **`1`** through **`60`** minutes.

The consoleTimeout interval is used only when **`consoleTimeout timeout`** *is* `enabled.`

Running Scripts of Administration Console Tasks

You can use scripts to expedite and automate Administration Console tasks. You can include any command that you enter in the Administration Console as part of a script. You can even script the entire system setup so that you can repeat it on other Switch 3900 and 9300 systems.

You create scripts in an ASCII-based line editor, such as *EMACS* or *vi* on a Trivial File Transfer Protocol (TFTP) server. To run them from the Administration Console, access the directory where your scripts are stored. When you write scripts, use the number or pound symbol (#) to identify comments in the script.

Running Script Files on the TFTP Server

You must run the script file in the directory in which the TFTP daemon is running on the remote host. Because TFTP provides no user authentication, the file must be publicly readable and writable. Otherwise, the TFTP server does not grant requests for file access.

1 To run a script, from the top level of the Administration Console, enter:

```
script
```

The system prompts you for the host IP address and file path for where you have stored the script that you want to run. Press Return or Enter at any prompt to accept the default or current value in brackets.

2 Enter the host IP address of the TFTP server on which the script resides.

3 Enter the full path of the script.

The task you that scripted is run in the Administration Console.

The example shows how you can script these tasks to initially configure your SuperStack II Switch 3900 system:

- Changing the serial port baud
- Setting the system name
- Assigning an IP address for management
- Checking the IP connection by pinging the system
- Enabling Spanning Tree Protocol on the system
- Setting up SNMP trap reporting

```
# This script performs some start-up configurations.
#
# Set the modem serial port baud rate.
#
system serialPort baudRate
9600 # modem serial port baud rate
#
# Set the system name
#
system name
Engineering SuperStack II 3900_4
#
# Assign an IP address to the SuperStack II 3900.
#
ip interface define
158.101.112.99 # IP address for the system
255.255.0.0 # subnet mask
#
# Enter the interface type (vlan or system)
#
ip interface summary
#
# Validate access to management workstation
#
ip ping
158.101.112.26 # management workstation address
#
```

```
# Enable the Spanning Tree Protocol
#
bridge stpState enabled
#
# Configure my node as an SNMP trap destination
#
snmp trap add
158.101.112.26 # management workstation address
all  # turn on all traps
q    # no more trap destinations
#
snmp trap display
#
```

Viewing More Levels of Menu Options

The outlining feature allows you to list the menu options that fall lower than the current menu in the hierarchy. The default displays up to three levels of options.

To display the outline of available options below the current menu, enter **`outline`** (or **`o`**).

To set how many levels that you see, add a number to the command. For example, to display two levels, enter:

```
outline 2
```

Logging Out of the Administration Console

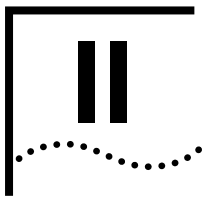
If you are accessing the system through the Console serial port, logging out returns you to the password prompt.

Top-Level Menu

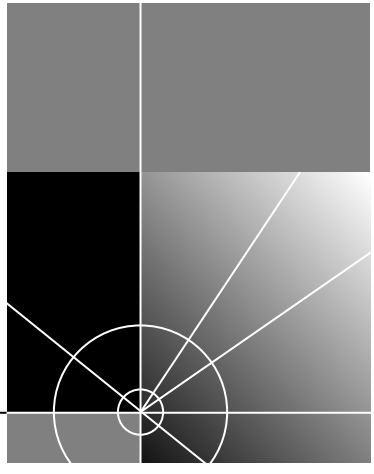
- system
- management (9300 only)
- ethernet
- bridge
- ip
- snmp
- script
- logout

1. To log out from the Administration Console, return to the top level by pressing Escape.
2. From the top-level menu, enter:

```
logout
```



SYSTEM-LEVEL FUNCTIONS



3 Configuring Management Access to the System

This chapter describes how to configure management access to your SuperStack® II Switch 3900 or 9300 system through one of two serial connection types or through a management interface. It also describes how to configure the system so that you can manage it using the Simple Network Management Protocol (SNMP). This chapter covers the following topics:

- About Management Access
- Setting Up the Serial Port
- Setting Up a Management Interface
- Setting Up SNMP on Your System

About Management Access

You can access the Administration Console in any of these ways:

- Directly through the Console port
- After you establish a management interface, through an SNMP-based network management application
- *In the Switch 9300 only,* from a PC or workstation, through the system Ethernet out-of-band port via a telnet session

Using a Serial Connection

Direct access through the Console port is often preferred because you can stay attached during system reboots.

For serial port pin-outs, *see the Getting Started Guide for your system.*

Serial connections are often more readily available at a site than Ethernet connections are. For a Macintosh computer or PC, use any terminal emulation program when you connect to the Console port. For a UNIX workstation, use an emulator such as tip.

Using a Management Interface

A management interface allows you to manage the system in band through an Ethernet switch port or out of band *(Switch 9300 only)* through the 10BASE-T port on the front panel. After you configure a management interface with a unique IP address, you can access the Administration Console using telnet from a host computer, or you can reach the SNMP agent from an external management application.

In-band or Out-of-band?

If you manage your system and its attached LANs over the same network that carries your regular data traffic, then you are managing your network *in band*. This kind of management is often the most convenient and inexpensive way to access your system. The disadvantage is that, if a fault occurs in your data network, you may not be able to diagnose the problem because in-band management requests travel over the same network.

Out-of-band management is not available on the Switch 3900. For the Switch 9300, if you define a management interface on a Gigabit Ethernet port, you are managing the system *in band.* If you are using a dedicated network for management data, then you are managing your network *out of band*. The out-of-band port on the Switch 9300 is the 10BASE-T port on the front panel.

If Spanning Tree is enabled on a port and the port is in the blocking state, you cannot use the in-band management protocol on that port.

See "Setting Up a Management Interface" on page 3-4 for details.

Setting Up the Serial Port

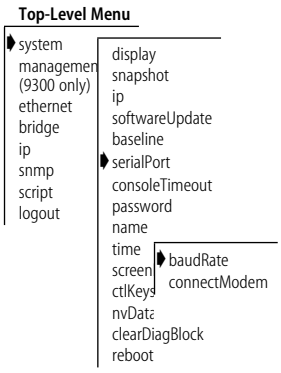
The system has one serial port that can be configured for terminal or modem connection.

Setting the Baud Rate

The default baud setting for the serial port is 9600. You can change the rate to match the port speed on your terminal or modem.

Baud setting changes take effect immediately after you confirm the change. Therefore, you must adjust the baud setting of your terminal or terminal emulator appropriately before you can reestablish communication using the terminal port.

When you change the baud rate to something other than 9600, the new setting becomes the new default even after you issue a **`system nvdata reset`** *command.*



1 To set the baud for the serial port, from the top level of the Administration Console, enter:

```
system serialPort baudRate
```

2 Enter the baud setting for the serial port.

The system supports these rates: 19200, 9600, 4800, 2400, and 1200.

The system response depends on the cable status. If the cable is connected to the terminal port when you set the baud for that port, the system displays the following message:

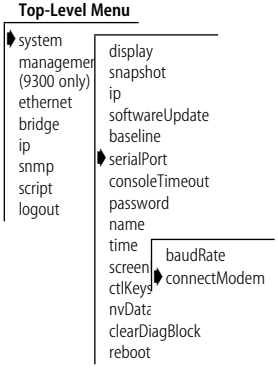
```
Changing the baud rate may cause a loss of communication
since you are currently connected via the serial port.

Are you sure you want to change the baud rate? (y/n):
```

- If you respond **y** (yes), the rate is changed immediately, and you lose the ability to communicate on the terminal port until you adjust the baud setting of your terminal or terminal emulator *(tip)* to match.
- If you respond **n** (no), the rate does not change, and the display returns to the previous menu.

Configuring the External Modem

You can configure the external modem by establishing a connection between your current Console session and the modem port.

When you have configured the external modem from the Administration Console, the system transmits characters that you have entered as output on the modem port. The system echoes characters that it receives as input on the modem port to the current Console session. The Console appears to be directly connected to the external modem.



1 To configure the modem port, from the top level of the Administration Console, enter:

```
system serialPort connectModem
```

You can now enter commands that support the appropriate parameters for your installation. All characters that you enter are transmitted to the modem port until you type the escape sequence described next.

2 When the modem is configured, enter the escape sequence **~]** with no intervening characters or spaces.

When you enter the escape sequence, the system breaks the connection to the modem serial and returns you to the previous menu.

Setting Up a Management Interface

The Internet Protocol (IP) is a standard networking protocol that is used for communications among various networking devices. To gain access to the system using TCP/IP or to manage the system using SNMP, you must set up an IP management interface for your system, as described in this section.

In-Band Management

If you are managing your network in band, you need to set up a management interface and at least one VLAN.

You can assign an IP interface to the default VLAN.

See Chapter 10 for information on how to define a VLAN. See Chapter 11 for information on how to set up an IP interface.

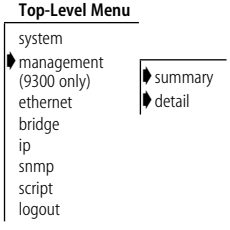
Out-Of-Band Management (Switch 9300 only)

If you are managing your Switch 9300 out of band, you first assign an IP address and subnet mask to the out-of-band management Ethernet port through the `ip` menu. The out-of-band management Ethernet port is the 10BASE-T port on the front of the system.

Displaying the Management Interface Statistics (Switch 9300 only)

For the Switch 9300, you can display summary or detailed information about the management interface configuration, including parameter settings.

To display summary or detail management interface information for the Switch 9300, from the top level of the Administration Console, enter:




```
management summary
```

or

```
management detail
```

The system displays the management interface information in the format that you specified.

For descriptions of the fields in the `management summary` *and* `detail` *displays, see Table 7-1.*

Sample Switch 9300 management interface summary display:

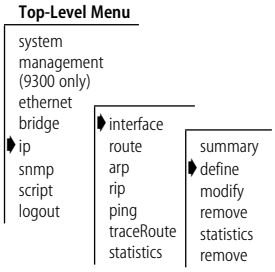
```
                                portLabel

                                    portType                portState
                                10BaseT(RJ45)                 on-line

                linkStatus          autoNegMode             autoNegState
                  disabled                  n/a                      n/a

              reqPortMode       actualPortMode          reqFlowControl
                   10half                10half                      n/a

          actualFlowControl             rxFrames                txFrames
                       n/a              3409497                     112

                  rxBytes             txBytes                   rxErrs
              1001791339               15469                        1

                   txErrs          noRxBuffers             txQOverflows
                        0                  n/a                      n/a

               macAddress
00-80-3e-46-43-4f
```

Sample Switch 9300 management interface detail display:

```
          rxFrames              rxBytes          rxFrameRate
           3412797           1002543264                  n/a

       rxByteRate      rxPeakFrameRate      rxPeakByteRate
              n/a                  n/a                  n/a

      noRxBuffers        alignmentErrs             fcsErrs
              n/a                    0                    0

            runts            fragments             jabbers
              n/a                  n/a                  n/a

        oversized       rxInternalErrs           rxDiscards
              n/a                    0              3287644

       rxUnicasts         rxMulticasts        rxMcastsOnly
              129              3412670                  n/a

      rxBroadcast              txFrames              txBytes
              n/a                  139                20472

      txFrameRate           txByteRate      txPeakFrameRate
              n/a                  n/a                  n/a

   txPeakByteRate         txQOverflows      excessCollision
              n/a                  n/a                    1

                       txInternalErrs      carrierSenseErr
                                    0                    0

       txDiscards           txUnicasts        txMulticasts
                0                  140                    2

     txMcastsOnly         txBroadcasts          collisions
              n/a                  n/a                  n/a

   lateCollisions       requestedState
              n/a              enabled

                            portLabel


                              portType            portState
                           10BaseT(RJ45)              on-line

       linkStatus           macAddress          autoNegMode
         disabled    00-80-3e-46-43-4f                  n/a

     autoNegState          reqPortMode       actualPortMode
              n/a                10half               10half

   reqFlowControl    actualFlowControl          paceAccess
              n/a                  n/a                  n/a
```

In-Band Management Interface

When you define an in-band management interface for the Switch 3900 or 9300, you specify several characteristics that are associated with that interface.



1 To assign an IP address to the in-band management port, from the top-level of the Administration Console, enter:

```
ip interface define
```

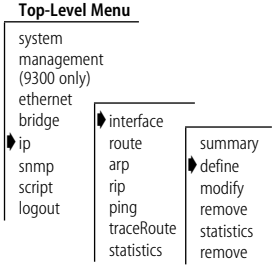
2 Enter the IP address for the in-band management port.

3 Enter the subnet mask. To accept the default or current subnet mask that the system displays in brackets, press Return or Enter.

4 For the in-band management port, enter **`vlan`** for the interface type.

Out-of-Band Management Interface (Switch 9300 only)

When you define an out-of-band management interface for the Switch 9300, you specify several characteristics that are associated with that interface.



1 To assign an IP address to the out-of-band management port, from the top level of the Administration Console, enter:

```
ip interface define
```

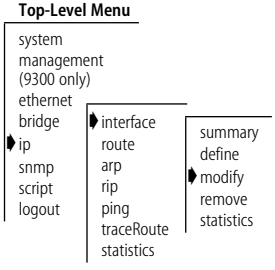
2 Enter the IP address for the out-of-band management port.

3 Enter the subnet mask. To accept the default or current subnet mask that the system displays in brackets, press the Return or Enter key.

4 For the out-of-band management port, enter **`system`** for the interface type.

Modifying a Management Interface

You can change the configuration of the management interface that you have already defined.



1. To modify a management interface, from the top level of the Administration Console, enter:

   `ip interface modify`

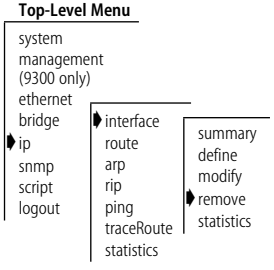
   You are prompted for the new interface values. Press Return or Enter at the prompts for which you do not want to change the value.

2. Modify the existing interface parameters by entering a new value at the prompt.

   You can monitor IP activity for your system by displaying the IP statistics at any time.

Removing a Management Interface

You may want to remove a management interface if you are no longer using it to route on the ports that are associated with the interface.



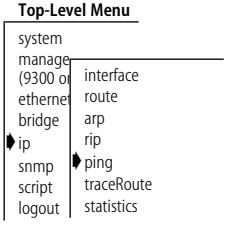
1. To remove a management interface definition, from the top level of the Administration Console, enter:

   `ip interface remove`

2. Enter the index number of the interface that you want to remove.

Pinging an IP Address

To determine whether an IP address is reachable, you can use the ping command from another station on your network.



1. To ping an IP station, from the top level of the Administration Console, enter:

   `ip ping`

2. Enter the IP address or hostname of the station that you want to ping.

   If the address or hostname is reachable, the system displays status information about the ICMP echo reply packets that it receives from the IP station. If you receive a response such as `Host is Unreachable` or `Host is Unresponsive`, be sure that you have defined the correct interface values and that you have the appropriate route defined to that network.

See "Using the Ping Function" on page 11-14 for more on pinging.

Setting Up SNMP on Your System

To manage the system from an external network management application, you must configure SNMP community strings and set up trap reporting, as described in this section.

You can manage the system using an SNMP-based external management application. This application (called the SNMP manager) sends requests to the system, where they are processed by the system's SNMP agent.

The SNMP agent provides access to the collection of information about the system. Your views of MIB information differ depending on the system SNMP management method that you choose.

In addition, an SNMP agent sends traps to an SNMP manager to report significant events.

Access to system information through SNMP is controlled by community strings.

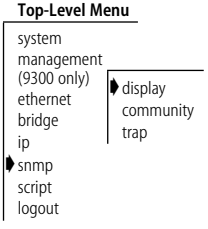
To manage the system with SNMP, you must use either an in-band management interface (Switch 3900 or 9300) or an out-of-band management interface (Switch 9300 only).

Configuring SNMP for System Management

To configure SNMP for system management with SNMP, you must:

- Assign an IP address
- Set the destination IP address to which the traps should be forwarded by the system agent

Displaying SNMP Settings



You can display the current SNMP configuration for community strings.

To display SNMP settings, enter the following command string from the top level of the Administration Console:

```
snmp display
```

Sample SNMP settings display:

```
Read-only community is public
Read-write community is private
```

Configuring Community Strings

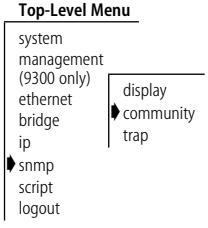
A community string is an octet string, included in each SNMP message, that controls access to system information. The internal SNMP agent internally maintains two community strings that you can configure:

- *Read-only* community strings, with the default access of "public"
- *Read-write* community strings, with the default access of "private"

When an SNMP agent receives an SNMP request, the agent compares the community string in the request with the community strings that are configured for the agent. SNMP *set* requests are valid only if the community string in the request matches the agent's *read-write* community. The SNMP *get* and *get-next* requests are valid if the community string in the request matches the agent's *read-only* or *read-write* community string.

Community string length

When you set a community string, you can specify any value up to 48 characters long.



1 To set a community string, from the top level of the Administration Console, enter:

```
snmp community
```

The system prompts you for a read-only community value and then for a read-write community value. If you do not want to change the value of a community string, press Return or Enter at either prompt.

2 At the read-only prompt, enter the new community string.

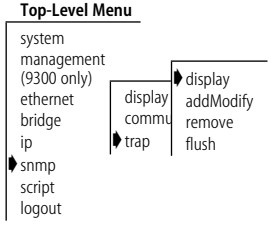
3 At the read-write prompt, enter the new community string.

```
Enter new read-only community [public]:
Enter new read-write community [private]: secret
```

Administering SNMP Trap Reporting

For network management applications, you can use the Administration Console to manually administer the trap reporting address information.

Displaying Trap Reporting Information



When you display the trap reporting information, the system shows you the SNMP traps and their currently configured destinations.

To display trap reporting information, from the top level of the Administration Console, enter:

```
snmp trap display
```

The system displays the trap settings.

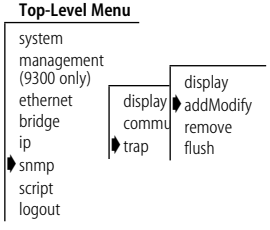
Sample trap settings display:

```
Trap Descriptions:
Trap#   Description
   1    MIB II: Coldstart
   2    MIB II: Link Down
   3    MIB II: Link Up
   4    MIB II: Authentication Failure
   5    Bridge MIB: New Root
   6    Bridge MIB: Topology Change
   7    S2 Systems MIB: System Overtemperature
   8    S2 Systems MIB: Power Supply Failure
   13   S2 Systems MIB: Address Threshold

Trap Destinations Configured:
   Address                          Trap Numbers Enabled
   158.101.112.3                    1-3, 6
```

Configuring Trap Reporting

You can add new trap reporting destination configurations and modify existing configurations. You can define up to 10 destination addresses and the set of traps that are sent to each destination address.

To add a new trap reporting destination configuration or modify a current one, follow these steps.



1. From the top level of the Administration Console, enter:

   `snmp trap addModify`

2. Enter the IP address (destination address) of the SNMP manager.
3. Enter one or more trap numbers or **`all`** for that destination.

   Separate a series of more than two trap numbers with a hyphen (-) and nonsequential trap numbers by commas.

The trap numbers that you enter allow the system to send the trap specified by that number to the destination address when the corresponding event occurs. Listed traps are not transmitted.

Example: Enter the trap destination address: **`158.101.222.3`**

```
Enter the trap numbers to enable (1-8,12-13|all) [1-8,12-23|all]:
all
```

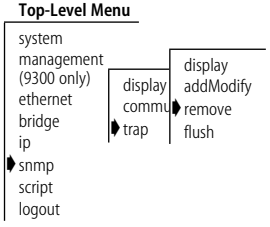
Address error If the destination address that you entered is not a valid end station, if a valid IP interface is not defined on the system, or if the agent does not have a route to the destination, the agent displays this message:

```
Trap address invalid or unreachable
```

If you see this message, confirm the IP address of the end station and that the end station is online.

Removing Trap Destinations

When you remove a destination, no SNMP traps are reported to that destination.



1 To remove a destination, from the top level of the Administration Console, enter:

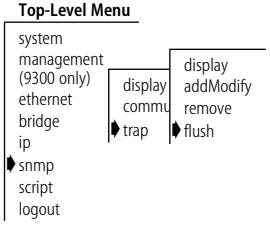
```
snmp trap remove
```

2 Enter the SNMP trap reporting destination address that you want to remove.

The system removes the destination address and displays the previous menu.

Flushing All SNMP Trap Destinations

When you flush the SNMP trap reporting destinations, you remove all trap destination address information for the SNMP agent.



1 To flush all SNMP trap reporting destinations, from the top level of the Administration Console, enter:

```
snmp trap flush
```

The following prompt appears:

```
Are you sure? (n/y) [y]:
```

2 Enter **y** (yes) or **n** (no).

If you enter **y**, the addresses are immediately flushed. If you enter **n**, the previous menu appears on the screen.

4 ADMINISTERING YOUR SYSTEM ENVIRONMENT

This chapter focuses on the administration of your SuperStack® II Switch 3900 and Switch 9300 system environment, including these tasks:

- Displaying the System Configuration
- Using the Snapshot Feature
- Setting Passwords
- Setting the System Name
- Changing the Date and Time
- Clearing the Diagnostic Block
- Rebooting the System

Displaying the System Configuration

Top-Level Menu

system	display
management (9300 only)	snapshot
ethernet	softwareUpdate
bridge	baseline
ip	serialPort
snmp	consoleTimeout
script	password
logout	name
	time
	screenHeight
	ctlKeys
	nvData
	clearDiagBlock
	reboot

The system configuration display provides software and hardware revisions, module status information, and warning messages for certain system conditions.

To display the configuration of a system, enter this command from the top level of the Administration Console:

```
system display
```

Sample Switch 9300 system configuration display:

```
SuperStack II Switch 9300 (rev 48.49) - System ID 7ed8ee
Base Software
Version 1.0.0 (beta 2) - Built 03/03/98 10:03:54 AM
System up time: 3 Days 15 Hours 45 Minutes 38 Seconds
Time in Service: 23 Days
                                          Rev Diagnostics  Serial
    1000BaseSX M/B, 9 MMF SC ports         01 Passed       2KCA000158
    1000BaseSX MZ, 3 MMF SC port           01 Passed       2KCA000158
    10BaseT OOB, 1 RJ45 port               01 Passed       2KCA000158

AP Memory Size     : 8 Mb
FP Memory Size     : 0 Mb
Flash Memory Size  : 2 Mb
Buffer Memory Size : 0 Mb
```

The display contains the following general system information:

- The system name
- The system ID
- The software version, build date, and time
- The system up time, which is the time since the last system reboot
- The time in service, which is the total amount of time that the system has been running
- Diagnostic information
- Memory size

Diagnostic messages A message appears in the display if any of the modules fails any of the diagnostic tests at start up.

Using the Snapshot Feature

The snapshot feature captures an image of all system display screens. The displays reflect the current values of all fields and counters at the time that you issue the command. You can select a summary display or a detail display. If a feature or protocol has only one display option (`display`), the system includes that image with both the summary and detail displays.

You specify whether you want the system to display the images of the summary or detail screens to the Console or to save the images of detail screens to a file on a host system. The system uses the Trivial File Transfer Protocol (TFTP) to transfer files to the host.

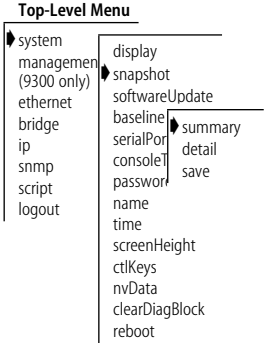
Creating Snapshot Files on the TFTP Server

Before you send the images to the file, you must create the file that will receive the snapshot images on the TFTP server. Because TFTP provides no user authentication, create the file on the server to be publicly readable and writable or the TFTP server does not grant requests for file access.

Displaying Snapshot Summary Screens

To display all system summary and display screens, from the top level of the Administration Console, enter:

```
system snapshot summary
```



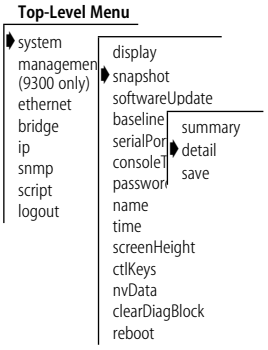
The summary displays appear on the screen.

Press Return or Enter to scroll through the images.

Displaying Snapshot Detail Screens

To display all system detail and display screens, from the top level of the Administration Console, enter:

```
system snapshot detail
```



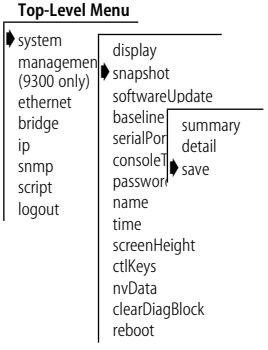
The detail displays appear on the screen.

Press Return or Enter to scroll through the images.

Saving Snapshot Detail Screens

You can tell the system to send detail screens to a file on the TFTP host that you specify. You supply the IP address of the host and the complete path to the file where you want to store the display images.

To save all system detail and display screens to a file on a host:



1. Create an empty file on the host that will store the system display images.
2. From the top level of the Administration Console, enter:

   ```
   system snapshot save
   ```

3. Enter the IP address of the host on which you want to save the display images.
4. Enter the complete path to the file that you created to contain the display images.

   As the system sends the files to the host, it displays the name of each display image that it transfers. When the transmission is complete, the system displays a message that the transfer is complete and displays the name of the system on which it stored the file.

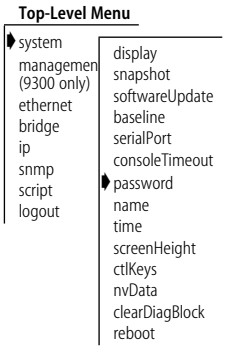
Setting Passwords

The Administration Console supports three levels of access: one for only browsing or viewing (*read*), one for configuring network parameters (*write*), and one for full system administration (*administer*).

Initial passwords

Because the initial passwords stored in the nonvolatile memory of the system are null for all access levels, press Return or Enter at the password prompt when you log on for the first time.

You can change passwords only if you enter the Console at the administer access level.



1 To set a password, from the top level of the Administration Console, enter:

```
system password
```

2 A prompt asks you to enter the password access level that you want to change. Enter one of the following commands:

- **`read`**
- **`write`**
- **`administer`**

3 At the prompt for your old password, enter the old password.

4 At the prompt for your new password, enter the new password.

The password can be no more than 32 characters long. It is case sensitive. To enter a null password, press the Return or Enter key.

5 Retype the new password for verification. The system does not display the password in any of the fields as you type.

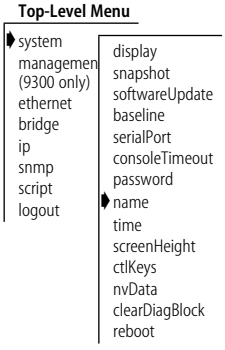
Example:

```
Select menu option (system): password
Password access level (read, write, administer) read
Old password:
New password:
Retype new password:
Administration console password has been successfully changed.
```

6 Repeat steps 1 through 5 for each level of password that you want to configure.

Setting the System Name

Give the system an easily recognizable and unique name to help you manage it. For instance, you can name the system according to its physical location, as in *SSII3900-ENGLAB*.



1 To name the system, from the top level of the Administration Console, enter:

```
system name
```

The system prompts you for the name:

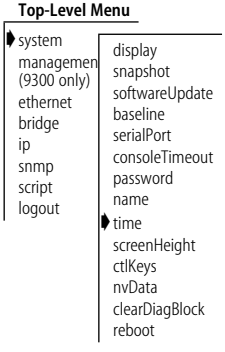
```
Enter new string (no spaces) [Switch3900]:
```

2 Enter a name that is both unique on the network and meaningful to you.

The new system name appears the next time that you display the system configuration.

Changing the Date and Time

The system's internal clock is initialized when shipped from the factory. You can display and change the system's current date and time.



1 To change the system's date or time, from the top level of the Administration Console, enter:

```
system time
```

The system displays the current date and time, and a prompt that asks whether you want to change the time, as shown here:

```
The current system time is 08/24/98 04:37:57 PM.
Do you want to change the system time (n,y) [y]:
```

2 Enter **y** (yes) or **n** (no) at the prompt.

If you respond **y**, the system prompts you for the correct date and time. If you respond **n**, the top-level menu appears.

3 Enter the correct date and time in this format:

```
mm/dd/yy hh:mm:ss xM
```

Table 4-1 lists the format variables.

Table 4-1 Date and Time Variables

Format	Description
first mm	month (**1–12**)
dd	date (**1–31**)
yy	last two digits of the year (**00–99**)
hh	hour (**1–12**)
second mm	minute (**00–59**)
ss	second (**00–59**)
xM	**AM** or **PM**

4 Press Enter or Return when you want the system to start keeping the time that you enter.

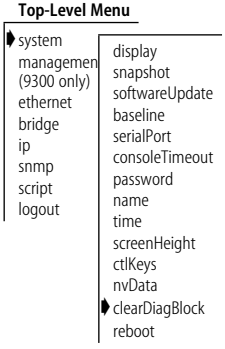
Example:

```
Enter the new system time (mm/dd/yy hh:mm:ss xM): 04/30/98
10:00:00 AM
Press RETURN at the exact time:
```

For information on Year 2000 compliance and 3Com products, visit the 3Com Year 2000 Web page:

http://www.3com.com/products/yr2000.html

Clearing the Diagnostic Block



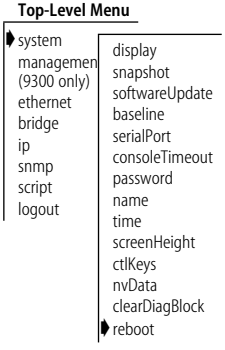
To keep diagnostic information about failed modules from accumulating in system display screens, from the top level of the Administration Console, enter:

```
system clearDiagBlock
```

The system immediately removes the diagnostic information about failed modules from the SNMP MIB *swSysDiagnosticsGroup*.

Rebooting the System

If your system is connected to the Administration Console by an external modem or through a telnet session, rebooting the system disconnects your session. To retain a connection to the Administration Console during reboots so that you can view diagnostic information, you must connect your system through the Console serial port.



1. To reboot the system, from the top level of the Administration Console, enter:

   ```
   system reboot
   ```

   The following message appears:

   ```
   Are you sure you want to reboot the system? (n,y):
   ```

2. Enter **y** (yes) or **n** (no).

   If you enter **y**, the system reboots. If you enter **n**, the previous menu appears.

5 BASELINING STATISTICS

This chapter describes how baselining statistics works in the SuperStack® II Switch 3900 and Switch 9300 system, as well as how to perform the following tasks:

- About Setting Baselines
- Displaying the Current Baseline
- Using the Set Command
- Enabling or Disabling Baselines

About Setting Baselines

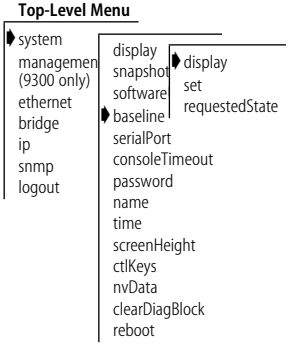
Normally, the system starts to compile statistics for MACs and ports when you turn it on. Baselining allows you to view compiled statistics over the period of time since you set a baseline.When you view statistics relative to a baseline, you can more easily evaluate recent activity in your system or on your network.

Baselining is maintained across Administration Console sessions. Statistics that you view after you set the baseline indicate that they are relative to the baseline. To view statistics as they relate only to the most recent power up, disable the baseline.

When you log out of an Administration Console session, the `baseline` *is maintained but the* `state` *is not. You must set the* `requestedState` *to* **`enable`** *when you log in.*

Baselining affects the statistics that are displayed for Ethernet ports and bridges.

Displaying the Current Baseline



You can display the current baseline to see when the baseline was last set and to determine if you need a newer baseline for viewing statistics.

To display the current baseline, from the top level of the Administration Console enter:

`system baseline display`

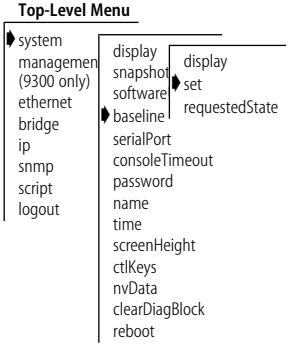
Example:

```
Baseline set at 4/30/98 10:42:52 AM is currently enabled.
```

If you have not yet set a baseline on the system, you see the following message:

```
A baseline has not yet been set.
```

Using the Set Command



This command resets the baseline counters to zero *(0).* The system maintains the accumulated totals since power up. The baseline is time-stamped.

To set a baseline, from the top level of the Administration Console, enter:

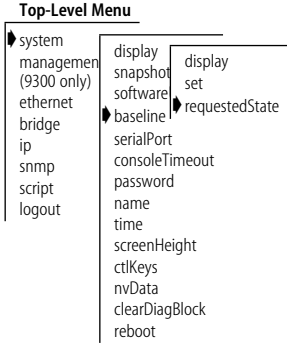
`system baseline set`

A message appears similar to the following:

```
Baseline set at 4/30/98 10:42:52 AM.
```

Baselining is automatically enabled when you set a baseline.

Enabling or Disabling Baselines



When you reenable a baseline, the counters return to the values that accumulated since the most recent baseline that you set. When you disable a baseline, the counters return to the total accumulated values since the last power up.

1 To enable or disable the current baseline, from the top level of the Administration Console, enter:

```
system baseline requestedState
```

2 Enter a new baseline state: **`disabled`** or **`enabled`**

The system confirms the new value.

Example:

```
Enter new value (disabled,enabled) [enabled]: disabled
Baseline set at 4/30/98 10:42:52 AM has been disabled.
```

6 Saving, Restoring, and Resetting Nonvolatile Data

This chapter describes the nonvolatile (NV) data in the SuperStack® II Switch 3900 and Switch 9300 systems, as well as how to perform the following tasks:

- Working with Nonvolatile Data
- Saving NV Data
- Restoring NV Data
- Examining a Saved NV Data File
- Resetting NV Data to Factory Defaults

Working with Nonvolatile Data

If you want to transfer NV data from one system to another, first save the system's NV data and then restore it as appropriate. You can save a configuration of the system for your reference and as a backup. You can also reset system data to its factory-configured values, if necessary.

During a save, the contents of NV memory are written to a disk file. All configurable parameters are saved in nonvolatile memory, including:

- System name
- System date and time
- Passwords
- Ethernet port labels
- Bridge and bridge port settings
- VLAN configurations
- IP interface configurations
- RIP mode setting
- SNMP community string settings
- SNMP trap destination configurations

The file also contains the following information, which is used to resolve any inconsistencies when NV data is restored:

- Software version number
- System ID
- Date and time of creation
- Type of configuration
- Data checksums

Saving NV Data

When the system saves NV data, it writes it to a file on a host computer (that is, a server) using the Trivial File Transfer Protocol (TFTP). You can then retrieve the information from the disk file when you use the **`restore`** command.

Creating NV Data Files on the TFTP Server

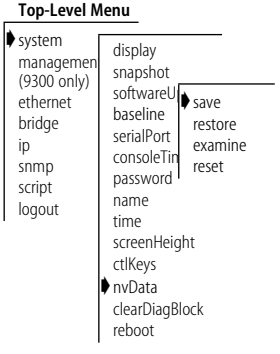
To store NV data, *before* you send the data, first create two files on the TFTP server:

- **Control file** — Use any filename that is meaningful to you. Example: `ctrlfile`
- **NV data file** — Use the control filename plus the **`.nvd`** extension. Example: `ctrlfile.nvd`

These files must reside in the host server directory in which the TFTP daemon is running.

Permissions

Because TFTP provides no user authentication, give *loose* permissions to the control file and the NV data file on the remote host; that is, make them publicly readable and writable. Otherwise, the TFTP server does not grant requests for file access.



1 To save NV data, from the top level of the Administration Console, enter:

```
system nvData save
```

The system prompts you for information about saving the data. To use the default or current value in brackets, press Return or Enter at the prompt. Any entry for IP address, filename, and user name becomes the new default.

2 Enter the IP address of the TFTP server.

3 Enter the full path of the control file. Even though the system prompt says `NV Control file,` enter the name of the control file without the extension.

4 Optionally, enter a label for the file.

Example:

```
Host IP Address [158.101.100.1]: 158.101.112.34
NV Control file (full pathname): systemdata
Enter an optional file label: Labdata
```

If the information is incorrect or if a connection cannot be made with the specified host, the system displays a message similar to this one:

```
Login incorrect.
Error: Could not open tftp session
```

If a session is successfully opened, a system message notifies you of the success or failure of your save, as in the following examples:

Success

```
System NV data successfully stored on host 158.101.112.34.
```

Failure

```
Saving system...transfer timed out.
Error - I/O error while writing nonvolatile data. Do you wish to
retry the save using the same parameters? (n,y) [y].
```

If you enter **y**, the system attempts to save the data as proposed.

If you enter **n**, the NV data is not saved and the previous menu appears.

The text of the failure message depends on the problem that the system encountered while saving the NV data.

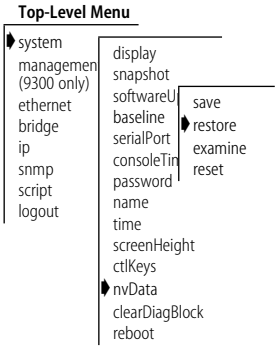
At the end of the save, the system display returns to the previous menu.

Sample retry request prompts:

```
Error - Checksum failure, configuration changed during save.
Error - Configuration not stored.
Do you wish to retry the save using the same parameters? (y/n):
```

Restoring NV Data

You can restore nvData regardless of the system configuration.



1. To restore the NV data, from the top level of the Administration Console, enter:

   `system nvData restore`

   The system prompts you to enter information for restoring the NV data that was saved to a file. Press Return or Enter at any prompt to accept the default or current value shown in brackets. Any entry for IP address, filename, and user name becomes the new default.

2. Enter the IP address of the host on which the NV data file resides.

3. Enter the full NV data file path and filename.

   If a session is successfully opened, the system reads the header information, compares the stored configuration to the current system configuration, and proposes a method of restoration based on one of the restoration rules described at the beginning of this section.

   The system prompts you to load the proposal.

   ```
   CAUTION - Restoring nonvolatile data may leave the system
   in an inconsistent state and therefore a reboot is
   necessary after each restore.
   Do you wish to continue? (y/n):
   ```

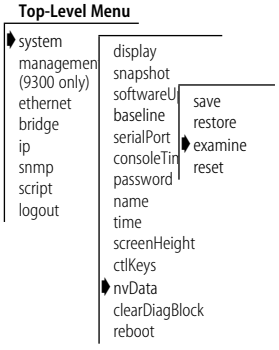
4. Enter **y** (yes) if you want to use the proposal. If you do not want to use the proposal, enter **n** (no).

   If you enter **y**, the system NV data is restored as proposed.

   If you enter **n**, the entire saved configuration is displayed for you to load manually.

5. At the end of a restore, press Return or Enter to reboot the system.

Examining a Saved NV Data File



After saving NV data to a file, you can examine the header information of that file.

1 To examine the file, from the top level of the Administration Console, enter:

```
system nvData examine
```

The system prompts you for information about examining a saved NV data file. Press Return or Enter at any prompt to accept the default or current value shown in brackets. Any entry for IP address, filename, and user name becomes the new default.

2 Enter the IP address of the host on which the NV data file resides.

3 Enter the full control file path.

If a session is successfully opened, the system displays the header information that corresponds to the filename entered.

Sample NV data file display:

```
Host IP address [158.101.117.250]:
NV Control file (full pathname) [nvData]:
Product ID 6, Product type 2:
System ID 127DA00
Saved 4/30/98 17:31:16 Version 2
Labelled: LabData
```

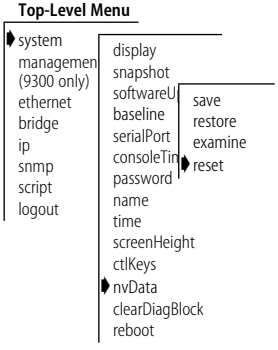
The system then displays the NV data menu options.

Resetting NV Data to Factory Defaults

At times you may not want to *restore* the system NV data. Instead, you may want to *reset* the values back to the factory defaults so that you can start configuring the system from the original settings.

CAUTION: *When you* **reset** *the NV data, the system returns all NV memory back to the factory defaults. Before you proceed, be sure that you want to* **reset** *your NV data. As a precaution, consider using* **save** *to save the current NV data to a file before you reset all values to the factory defaults.*

To reset all the NV data on the system to the original factory default values, follow these steps.



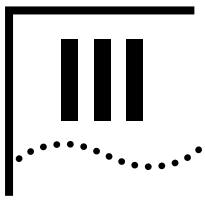
1 From the top level of the Administration Console, enter.

```
system nvData reset
```

The system displays the following prompt:

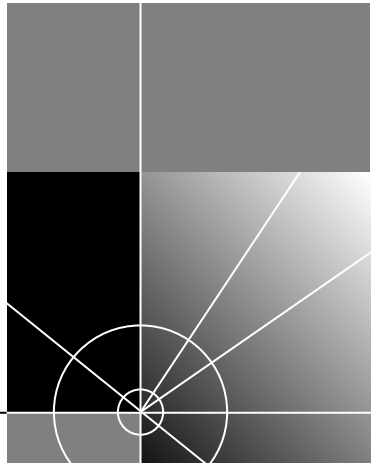
```
Resetting nonvolatile data may leave the system in an
inconsistent state and therefore a reboot is necessary
after each reset.
Do you wish to continue (n,y) [y]:
```

2 Confirm that you want to reset NV data by entering **y** (yes) at the prompt. If you enter **y** (yes), the system reboots and all settings on the system return to their factory defaults. If you enter **n** (no), the system displays the previous menu.



ETHERNET PARAMETERS

Chapter 7 Administering Ethernet Ports



7 ADMINISTERING ETHERNET PORTS

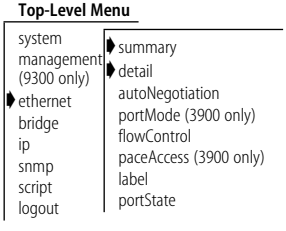
This chapter describes how to perform these tasks on the SuperStack® II Switch 3900 and Switch 9300 systems:

- Displaying Ethernet Port Information
- Enabling or Disabling Autonegotiation
- Setting the Port Mode (Switch 3900 only)
- Setting Flow Control
- Enabling and Disabling PACE (Switch 3900 only)
- Labeling an Ethernet Port
- Enabling and Disabling Ethernet Ports

Displaying Ethernet Port Information

You can display a summary of Ethernet port information or a detailed report. When you display a summary, you view the port's label and status, as well as the most pertinent statistics about general port activity and port errors. The detailed display of Ethernet port information includes the information in the summary and additional Ethernet port statistics, such as collision counters.

To display Ethernet port statistics relative to a baseline, see Chapter 5.



1 To display information about Ethernet ports, from the top level of the Administration Console, enter:

```
ethernet summary
```

or

```
ethernet detail
```

2 Enter one or more port numbers or **all**

The system displays the port information in the format that you specified.

Sample Ethernet port summary display:

```
port                                portLabel
   1
   3

port                                portType            portState
   1                             1000BaseSX(SC)           on-line
   3                             1000BaseSX(SC)          off-line

port           linkStatus          autoNegMode         autoNegState
   1              enabled              disable             disabled
   3             disabled              disable             disabled

port          reqPortMode        actualPortMode       reqFlowControl
   1             1000full             1000full                  off
   3             1000full             1000full                  off

port    actualFlowControl             rxFrames             txFrames
   1                  off              1414120                    4
   3                  off                    0                    1

port              rxBytes              txBytes              rxErrs
   1            356146128                  288                 n/a
   3                    0                   72                 n/a

port               txErrs          noRxBuffers         txQOverflows
   1                  n/a                    0                    0
   3                  n/a                    0                    0

port           macAddress
   1    00-80-3e-46-43-4f
   3    00-80-3e-46-43-51
```

Sample Ethernet port detail display:

```
port            rxFrames            rxBytes          rxFrameRate
   1             1419896          357608603                   25
   3                   0                  0                    0

port          rxByteRate      rxPeakFrameRate       rxPeakByteRate
   1                7934                 3288               989842
   3                   0                    0                    0

port         noRxBuffers       alignmentErrs             fcsErrs
   1                   0                 n/a                    0
   3                   0                 n/a                    0

port               runts           fragments             jabbers
   1                   0                   0                    0
   3                   0                   0                    0

port           oversized       rxInternalErrs          rxDiscards
   1                   0              101102                  n/a
   3                   0                   0                  n/a

port          rxUnicasts        rxMulticasts        rxMcastsOnly
   1              313859             1004955               74160
   3                   0                   0                   0

port         rxBroadcast            txFrames             txBytes
   1              930933                   4                 288
   3                   0                   1                  72

port         txFrameRate          txByteRate      txPeakFrameRate
   1                   0                   0                    0
   3                   0                   0                    0

port       txPeakByteRate        txQOverflows      excessCollision
   1                  14                   0                  n/a
   3                   7                   0                  n/a

port                                txInternalErrs      carrierSenseErr
   1                                             0                  n/a
   3                                             0                  n/a

port          txDiscards          txUnicasts        txMulticasts
   1                   0                   0                    4
   3                   0                   0                    1

port        txMcastsOnly        txBroadcasts          collisions
   1                   4                   0                  n/a
   3                   1                   0                  n/a

port       lateCollisions      requestedState
   1                  n/a             enabled
   3                  n/a             enabled

port                                 portLabel
   1
   3

port                                      portType           portState
   1                                 1000BaseSX(SC)             on-line
   3                                 1000BaseSX(SC)            off-line

port          linkStatus             macAddress         autoNegMode
   1             enabled    00-80-3e-46-43-4f              disable
   3            disabled    00-80-3e-46-43-51              disable

port        autoNegState         reqPortMode       actualPortMode
   1            disabled            1000full             1000full
   3            disabled            1000full             1000full

port       reqFlowControl    actualFlowControl          paceAccess
   1                  off                  off                  n/a
   3                  off                  off                  n/a
```

Table 7-1 describes the information provided about an Ethernet port.

Table 7-1 Fields for Ethernet Port Attributes

Field	Description
actualPortMode	Actual operating port mode. If autonegotiation is *enabled*, the value is the autonegotiated setting. If autonegotiation is *disabled*, the value is the user-selected port mode.
alignmentErrs	Number of frames received by this port that are not an integral number of octets in length and do not pass the FCS check
autoNegMode	Autonegotiation mode configured for port. Possible values are *enable* and *disable*.
autoNegState	Current negotiation state. Possible values are *disabled*, *configuring*, *completed*, and *failed*.
carrierSenseErr	Number of frames discarded because the carrier sense condition was lost while attempting to transmit a frame from this port
collisions	Number of collisions detected on this port
excessCollision	Number of frames that could not be transmitted on this port because the maximum allowed number of collisions was exceeded
excessDeferrals	Number of frames that could not be transmitted on this port because the maximum allowed deferral time was exceeded
fcsErrs	Number of frames received by this port that are an integral number of octets in length but do not pass the FCS check
flowControl	Flowcontrol mode for the configured port.
lateCollisions	Number of times that a collision was detected on this port later than 512 bit-times into the transmission of a frame
lengthErrs	Number of frames received by this port that are longer than 1518 bytes or shorter than 64 bytes
linkStatus	Boolean value indicating the current state of the physical link status for this port (either *enabled* or *disabled*)
macAddress	The MAC address of this port
noRxBuffers	Number of frames that were discarded because no buffer space was available
portLabel	User-defined name for the port. The maximum allowable length of the string is 32 characters, including the null terminator.
portState	Current software operational state of this port. Possible values are *on-line* and *off-line*.
portType	Specific description of this port's type.
requestedState	Configurable parameter that is used to enable or disable this port. The default is *enabled*.

(continued)

Table 7-1 Fields for Ethernet Port Attributes (continued)

Field	Description
reqPortMode	Configurable parameter that is used to set the port mode.
rxBroadcast	Number of broadcasts received.
rxByteRate	Average number of bytes received per second by this port during the most recent sampling period
rxBytes	Number of bytes received by this port, including framing characters. Summary display only.
rxErrs	Sum of all receive errors that are associated with this port
rxFrameRate	Average number of frames that were received per second by this port during the most recent sampling period. Sampling periods are 1 second long and not configurable.
rxFrames	The number of frames that were copied into receive buffers by this port
rxInternalErrs	Number of frames that were discarded because of an internal error during reception
rxMCastsOnly	Number of multicast frames received.
rxMulticasts	Number of multicast frames that were delivered to a higher-level protocol or application by this port
rxPeakByteRate	Peak value of ethernetPortByteReceiveRate for this port since the station was last initialized
rxPeakFrameRate	Peak value of ethernetPortFrameReceiveRate for this port since the station was last initialized
rxUnicasts	Number of unicast (nonmulticast) frames that were delivered by this port to a higher-level protocol or application
txByteRate	Average number of bytes that were transmitted per second by this port during the most recent sampling period
txBytes	Number of bytes that were transmitted by this port, including framing characters
txDiscards	Number of transmitted frames that were discarded because the port was disabled
txErrs	Sum of all transmit errors that are associated with this port (summary report only)
txFrameRate	Average number of frames that were transmitted per second by this port during the most recent sampling period. Sampling periods are 1 second long and not configurable.
txFrames	The number of frames that were transmitted by this port
txInternalErrs	Number of frames that were discarded because of an internal error during transmission
txMcastsOnly	Number of multicast frames transmitted.

(continued)

Table 7-1 Fields for Ethernet Port Attributes (continued)

Field	Description
txMulticasts	Number of multicast frames that are queued for transmission by a higher-level protocol or application, including those not transmitted successfully
txPeakByteRate	Peak value of ethernetPortByteTransmitRate for this port since the station was last initialized
txPeakFrameRate	Peak value of ethernetPortFrameTransmitRate for this port since the station was last initialized
txQOverflows	The number of frames that were lost because the transmit queue was full
txUnicasts	Number of unicast (nonmulticast) frames that are queued for transmission by a higher-level protocol or application, including frames not transmitted successfully

Frame processing and Ethernet statistics

All frames on the Ethernet network are received promiscuously by an Ethernet port. However, frames can be discarded for either of the following reasons:

- There is no buffer space available.
- The frame is in error.

Figure 7-1 shows the order in which these discard tests are made.

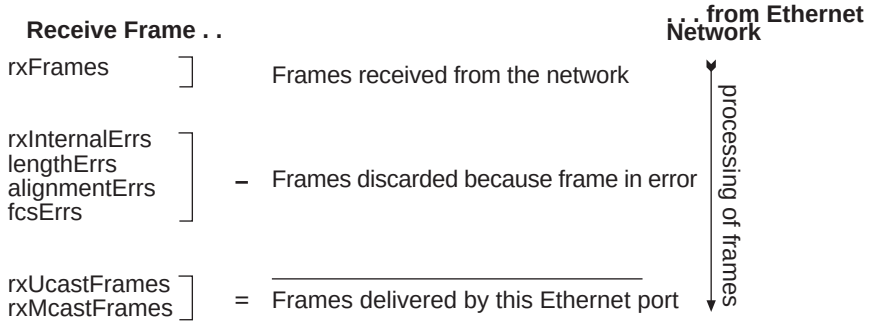


Figure 7-1 How Frame Processing Affects Ethernet Receive Frame Statistics

Frames are delivered to an Ethernet port by bridge, router, and management applications. However, a transmitted frame can be discarded for any of the following reasons:

- The Ethernet port is disabled.
- There is no room on the transmit queue.
- An error occurred during frame transmission.

Figure 7-2 shows the order in which these discard tests are made.

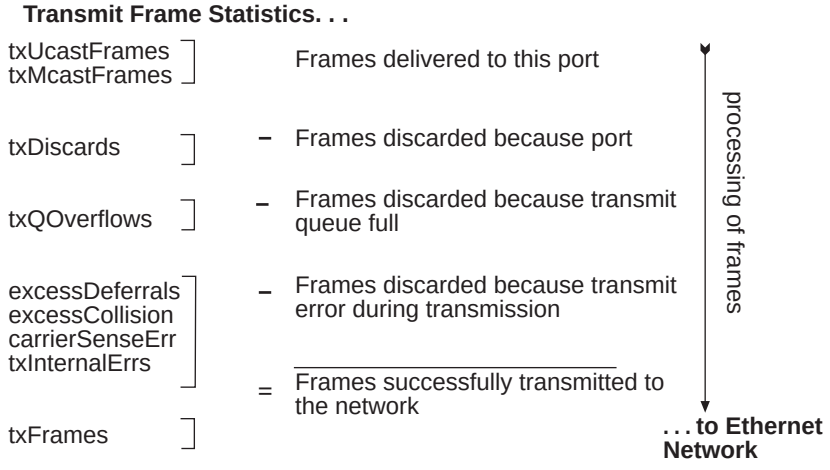


Figure 7-2 How Frame Processing Affects Ethernet Transmit Frame Statistics

Enabling or Disabling Autonegotiation

The autonegotiation feature determines whether some port types automatically negotiate certain attributes with the receiving device. Table 7-2 lists the SuperStack II Switch 3900 and 9300 port types, whether they support autonegotiation, which features they negotiate, and the default values for negotiable attributes.

In some instances, autonegotiation may not properly detect the remote port speed. In most cases this is due to the way the vendor of the remote device implemented either autonegotiation or a change in port speed. If autonegotiation does not properly detect the port speed, manually set the port speed and duplex mode.

Table 7-2 Port Types and Autonegotiation Attributes

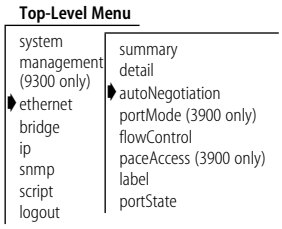
Port Type	Supports Autonegotiation?	Negotiable Attributes	Default Values for Negotiable Attributes
10/100BASE-TX (Switch 3900 only)	Yes	Port speed	10 Mbps
		Duplex mode	Half-duplex mode
1000BASE-SX	Yes	Duplex mode*	
		Flow control	On
1000BASE-LX	Yes	Duplex mode*	
		Flow control	On

* The 1000BASE-SX and 1000BASE-LX duplex mode is currently fixed at full-duplex. Both link partners must be set to full-duplex or the link does not come up.

When you enable autonegotiation on a 10/100BASE-TX port, you set this feature for both port speed and duplex mode. To change the value of one of these attributes but not the other, see the **`portMode`** command, later in this chapter.

If autonegotiation is enabled for a Gigabit Ethernet port, receive flow control is always configured.

Default Autonegotiation is *enabled* by default on those ports that support it.



1 To enable or disable autonegotiation, from the top level of the Administration Console, enter:

```
ethernet autoNegotiation
```

2 Enter one or more port numbers or **all**.

After you have selected the ports, the system prompts you to enable or disable autonegotiation on each selected port.

Example:

```
Select Ethernet port(s) (1-39|all): all
Port 1 - Enter new value (enable,disable) [enable]: enable
Port 2 - Enter new value (enable,disable) [enable]: enable
Port 3 - Enter new value (enable,disable) [enable]: enable
Port 4 - Enter new value (enable,disable) [enable]: enable
Port 5 - Enter new value (enable,disable) [enable]: disable
Port 6 - Enter new value (enable,disable) [enable]: disable
```

Setting the Port Mode (Switch 3900 only)

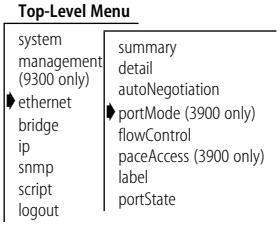
This command changes the port speed and duplex mode for the SuperStack II Switch 3900 10/100BASE-TX ports.

Table 7-3 lists the port mode options available for each port type.

Table 7-3 Port Mode Options

Port Type	Port Mode Options	Option Types	Default
10/100BASE-TX	100full	100 Mbps, full-duplex mode	10half
	100half	100 Mbps, half-duplex mode	
	10full	10 Mbps, full-duplex mode	
	10half	10 Mbps, half duplex mode	

CAUTION: *When you configure full-duplex mode, configure both the sending and the receiving devices.*



1 To change the port speed or duplex mode on a Fast Ethernet port, from the top level of the Administration Console, enter:

```
ethernet portMode
```

2 Enter one or more port numbers or **all**.

After you have selected the ports, the system prompts you to enter the port mode.

The following message appears on the screen:

```
Warning - The device connected to each port must be configured for
the same port mode. If the port speeds differ, the link will not
come up. If the duplex modes differ, excessive collisions will
occur.
```

If autonegotiation is enabled, the following message also appears:

```
Warning – Ethernet port 1 has auto-negotiation enabled. The
portMode selection will not take effect until
auto-negotiation is disabled for this port.
```

In the next example, ports 1, 2, 3, and 4 are 10/100BASE-TX ports, which include the 10Mbps and duplex options.

```
Select Ethernet port(s) (1-39|all) [1-6]: 1-4
Port 1 - Enter new value (10half,10full,100half,100full)
[10half]: 100full
Port 2 - Enter new value (10half,10full,100half,100full)
[10half]: 100full
Port 3 - Enter new value (10half,10full,100half,100full)
[10half]: 10full
Port 4 - Enter new value (10half,10full,100half,100full)
[10half]: 100full
```

Setting Flow Control

The flow control feature affects port characteristics that determine whether the port can respond to or generate flow control packets. These characteristics include:

- Whether a port can decrease the frequency with which it sends packets to a receiving device if that device cannot receive packets that are being sent to it too rapidly
- Whether a port can send flow control packets to a sending device and ask the sending device to decrease the frequency with which it is sending packets to the port

On Gigabit Ethernet ports, separate flow control parameters are available that determine whether a port can send flow control packets or respond when it receives a flow control packet.

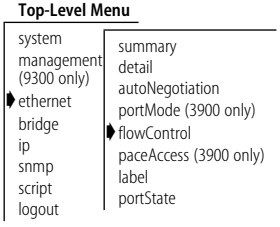
Table 7-4 lists the flow control options and the ports on which they are available.

Table 7-4 Flow control Options

Flow Control Option	Description	Available on These Port Types
on	The port recognizes flow control packets and can generate flow control packets.	■ Fast Ethernet ■ Gigabit Ethernet
off	The port ignores flow control packets that it receives and does not transmit them.	■ Fast Ethernet ■ Gigabit Ethernet
rxOn	The port receives and recognizes flow control packets. The port does not transmit or generate flow control packets.	■ Gigabit Ethernet
txOff	The port transmits and can generate flow control packets. The port ignores flow control packets that it receives	■ Gigabit Ethernet

The system does not count flow control packets in either receive or transmit statistics.

Default The default flow control option for all ports is *off*.



1 To set a flow control option, from the top level of the Administration Console, enter:

`ethernet flowControl`

2 Enter one or more port numbers or **`all`**

After you select the ports, the system prompts you to enter the flow control mode for each port.

Example for three Gigabit Ethernet ports (the maximum number of Gigabit Ethernet ports on a Switch 3900):

```
Select menu option (ethernet): flowControl
Select Ethernet port(s) (1-3|all) [1-3]: all
Port 1 - Enter new value (on,off) [on]:
Port 2 - Enter new value (on,off) [on]: off
Port 3 - Enter new value (on,off) [on]: off
Port 4 - Enter new value (on,off) [on]: on
```

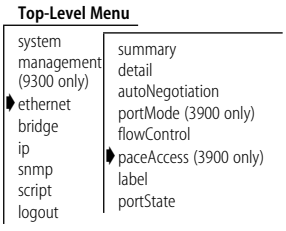
Enabling and Disabling PACE (Switch 3900 only)

The 3Com *PACE*™ technology is designed to provide reliable timing, optimal LAN bandwidth usage, and data prioritization for time-sensitive multimedia and real-time applications as well as for data-only applications.

You can configure the Ethernet ports on your system to support the PACE Interactive Access feature, which ensures reliable timing by preventing excessive Ethernet network jitter (the variation in the timing of packet delivery that can cause garbled sound, jerky images, and delays).

PACE Interactive Access:

- Employs a "back-off" algorithm that enables your system to control the flow of traffic on a point-to-point link with an end station. If there is congestion, the switch holds the packets.
- Avoids repetitive collisions and prevents an end station from "capturing" the link. (With conventional Ethernet, a packet collision can cause the last station that transmitted successfully to monopolize Ethernet access and cause delays.)



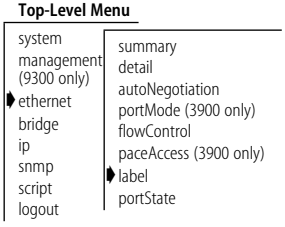
To set the PACE feature, from the top level of the Administration Console, enter:

```
ethernet paceAccess
```

1. Enter one or more port numbers or **all**
2. Enter the PACE mode for the ports that you specified: **on** or **off**

Labeling an Ethernet Port

Port labels serve as useful reference points and as an accurate way to identify your ports for management. Consider labeling your Ethernet ports so that you can easily identify the type of device that is attached to each port (for example, LAN, workstation, server).



1. To label an Ethernet port, from the top level of the Administration Console, enter:

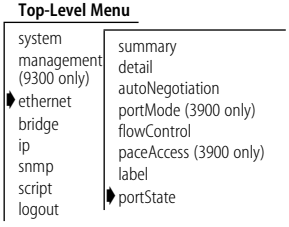
   `ethernet label`

2. Enter one or more port numbers or **`all`**
3. Enter the label for each port that you specified.

   Port labels can include up to 32 ASCII characters. The new port label appears the next time that you display information for that port.

Enabling and Disabling Ethernet Ports

You can *enable* (place online) or *disable* (place off-line) Ethernet ports with this command. When an Ethernet port is *enabled,* frames are transmitted normally over that port. When an Ethernet port is *disabled,* the port neither sends nor receives frames.

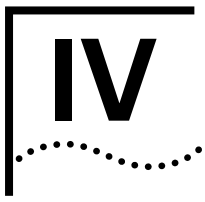


1. To enable or disable an Ethernet port, from the top level of the Administration Console, enter:

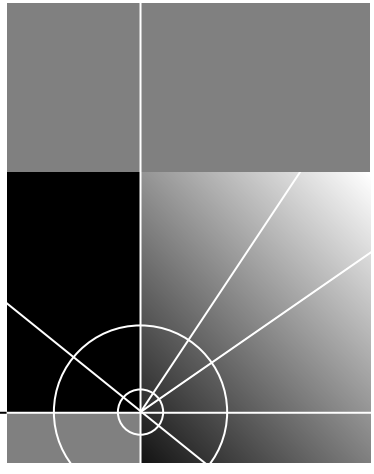
   `ethernet portState`

2. Enter the ports that you want to enable or disable.
3. Enter **`enabled`** or **`disabled`** for each Ethernet port that you specified.

   The *portState* value in the summary and detail displays reports *online* for all enabled ports displayed and *off-line* for all disabled ports displayed.



BRIDGING PARAMETERS



8 ADMINISTERING THE BRIDGE

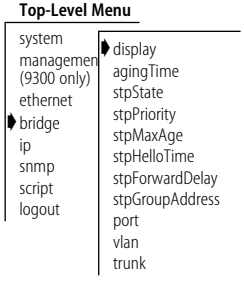
This chapter describes how to view the bridge setup on the SuperStack® II Switch 3900 and 9300 systems and how to configure the following bridge-level parameters:

- Displaying Bridge Information
- Setting the Aging Time
- Administering STP Bridge Parameters
- Administering Trunks

For information about configuring bridge ports, see Chapter 9. For information about creating VLANs for a bridge, see Chapter 10.

Displaying Bridge Information

You can display information about the bridge. The display includes bridge statistics (such as topology change information) and configurations for the bridge and Spanning Tree topology.



To display bridge information, from the top level of the Administration Console, enter:

```
bridge display
```

The system displays information about the bridge.

Sample bridge information display:

```
          stpState                timeSinceLastTopologyChange
           enabled             98 days 15 hrs 44 mins 21 secs

topologyChangeCount   topologyChangeFlag     BridgeIdentifier
                  9                 false    8000 00803e46434f

     designatedRoot      stpGroupAddress         bridgeMaxAge
8000 00803e028e16    01-80-c2-00-00-00                   20

            maxAge      bridgeHelloTime            helloTime
                20                    2                    2

     bridgeFwdDelay         forwardDelay             holdTime
                15                   15                    1

           rootCost             rootPort             priority
                31                    1               0x8000

         agingTime                 mode        addrTableSize
                300          transparent                  n/a

       addressCount        peakAddrCount        addrThreshold
                n/a                  n/a                  n/a

         lowLatency          bufferLimit
                n/a                  n/a
```

Each item in the bridge parameter display is described in Table 8-1.

Table 8-1 Bridge Attributes

Parameter	Description
addressCount	Number of addresses in the bridge address table
addrTableSize	Maximum number of addresses that will fit in the bridge address table
addrThreshold	Reporting threshold for the total number of addresses known on this bridge. When this threshold is reached, the system generates the SNMP trap addressThresholdEvent. The range of valid values for setting this object is between 1 and the value reported by the addressTableSize attribute +1.
agingTime	Time-out period in seconds (between 10 and 32267) for aging out dynamically learned forwarding information. The default value is *300* seconds (5 minutes).
bridgeFwdDelay	Forward delay value used when this bridge is the root bridge. This value sets the amount of time that a bridge spends in the "listening" and "learning" states. The default value is *15* seconds.
bridgeHelloTime	Hello time value, used when this bridge is the root bridge. This value is the time that elapses between the configuration messages generated by a bridge that assumes itself to be the root. The default value is *2* seconds.
BridgeIdentifier	Bridge identification. It includes the bridge priority value and the MAC address of the lowest numbered port. Example: 8000 00803e003dc0).
bridgeMaxAge	Maximum age value, used when this bridge is the root bridge. This value determines when the stored configuration message information is too old and is discarded. The default value is *20* seconds.
designatedRoot	Root bridge identification. It includes the root bridge's priority value and the MAC address of the lowest numbered port on that bridge. Example: 8000 00803e001520.
forwardDelay	The time that a bridge spends in the "listening" and "learning" states
helloTime	The time that elapses between the configuration messages generated by a bridge that assumes itself to be the root

(continued)

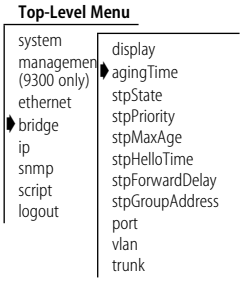
Table 8-1 Bridge Attributes (continued)

Parameter	Description
holdTime	Minimum delay time between sending BPDUs (topology change Bridge Notification Protocol Data Units)
maxAge	The maximum age value at which the stored configuration message information is judged to be too old and is discarded. This value is determined by the root bridge.
peakAddrCount	Peak value of addressCount
priority	Configurable value that is appended as the most significant portion of a bridge identifier
rootCost	Cost of the best path to the root from the root port of the bridge. For example, one determining factor of cost is the speed of the network interface: the faster the speed, the smaller the cost.
rootPort	Port with the best path from the bridge to the root bridge
stpGroupAddress	Address to which the bridge listens when receiving STP information
stpState	Configurable parameter that provides the state of the bridge (that is, whether Spanning Tree is *enabled* or *disabled* for that bridge). The default value is *disabled*.
timeSinceLastTopologyChange	Time elapsed (in hours, minutes, and seconds) since STP last reconfigured the network topology.
topologyChangeCount	Number of times that STP has reconfigured the network topology.
topologyChangeFlag	Indicates whether the bridge topology is currently changing (`true`) or not changing (`false`).

Setting the Aging Time

The bridge aging time is the maximum period (in seconds) for aging out dynamically learned forwarding information. This parameter allows you to configure the switching module to age addresses in a timely manner, without increasing packet flooding.

Default The default value is *300* seconds, which is 5 minutes.



1 To set the bridge aging time, from the top level of the Administration Console, enter:

```
bridge agingTime
```

2 Enter the aging time value. The values can range from *10* to *32,267* seconds.

Administering STP Bridge Parameters

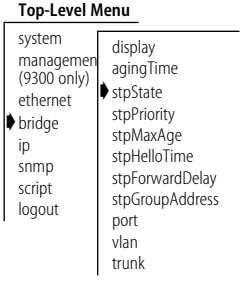
You can enable or disable the Spanning Tree Protocol on the system and set the following STP bridge parameters: priority, maximum age, hello time, forward delay, and group address.

Enabling and Disabling STP on a Bridge

When Spanning Tree Protocol is *disabled* on the system, the bridge does not participate in the Spanning Tree algorithm.

Default The default value is *disabled*.

To enable or disable Spanning Tree Protocol on one or more bridges in the system, follow these steps.



1 From the top level of the Administration Console, enter:

```
bridge stpState
```

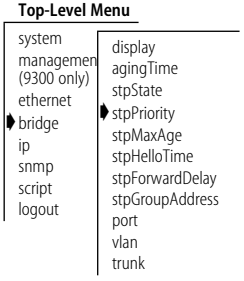
2 Enter the STP state: **`enabled`** or **`disabled`**

Setting the Bridge Priority

The bridge priority influences the choice of the root bridge and the designated bridge. The *lower* the bridge's priority number, the *more likely* it is that the bridge will be chosen as the root bridge or a designated bridge.

Bridge priority values

The bridge priority value is appended as the most significant portion of a bridge identifier (for example: `8000 00803e003dc0`). It is a 2-octet value.



1 To configure the STP bridge priority, from the top level of the Administration Console, enter:

```
bridge stpPriority
```

2 Enter the priority value for each bridge that you specified.

If your configuration was successful, the previous menu appears on the screen.

If the configuration was not successful, the system notifies you that your changes failed, and you can try to reenter your changes.

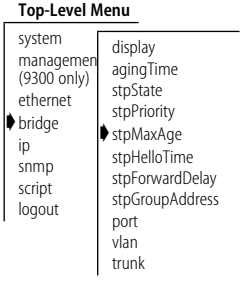
Setting the Bridge Maximum Age

The bridge maximum age determines when the stored configuration message information is judged to be too old and is discarded from the bridge's memory.

When the Spanning Tree Protocol is configured properly, the maximum age value should ideally never be reached. If the value is too small, then the Spanning Tree Protocol may reconfigure the topology too often, causing temporary loss of connectivity in the network. If the value is too large, the network may take longer than necessary to adjust to a new Spanning Tree configuration after a topology change such as the restarting of a bridge.

Maximum age recommended value

A conservative value is to assume a delay variance of *2* seconds per hop. The recommended value is *20* seconds.



1 To configure the bridge maximum age, from the top level of the Administration Console, enter:

```
bridge stpMaxAge
```

2 Enter the STP bridge max age value for each bridge that you selected.

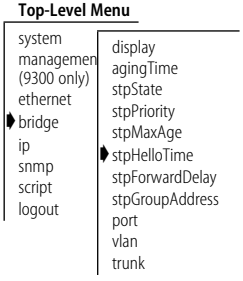
If your configuration was successful, the system returns you to the previous menu. If the configuration was not successful, the system alerts you that your changes failed, and you can try to reenter your changes.

Setting the Bridge Hello Time

Hello time is the period between the configuration messages generated by a root bridge. If the probability of losing configuration messages is high, shortening the time makes the protocol more robust. On the other hand, lengthening the time lowers the overhead of the algorithm.

Hello time recommended value

The recommended time is *2* seconds.



1 To configure the bridge hello time, from the top level of the Administration Console, enter:

```
bridge stpHelloTime
```

2 Enter the bridge hello time value for each bridge that you selected.

If the configuration was successful, the previous menu appears on the screen.

If the configuration was not successful, you are notified that your changes failed, and you can try to reenter those changes.

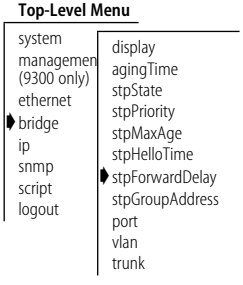
Setting the Bridge Forward Delay

The forward delay value specifies the amount of time that a bridge spends in the "listening" and "learning" states. This value temporarily prevents a bridge from starting to forward data packets to and from a link until news of a topology change has spread to all parts of a bridged network. This delay gives all the links that need to be turned off in the new topology enough time to turn off before the new links are turned on.

Setting the value too low can result in temporary loops as the Spanning Tree algorithm reconfigures the topology. On the other hand, setting the value too high can lead to a longer wait as the Spanning Tree Protocol reconfigures the topology.

Forward delay recommended value

The recommended value is *15* seconds.



1 To configure the forward delay, from the top level of the Administration Console, enter:

```
bridge stpForwardDelay
```

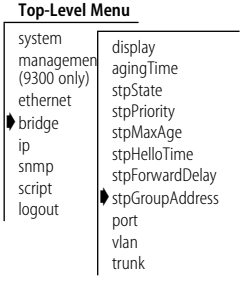
2 Enter the forward delay value for each bridge that you selected.

If your configuration was successful, the previous menu appears on the screen. If the configuration was not successful, the system notifies you that your changes failed, and you can try to reenter your changes.

Setting the STP Group Address

The STP group address is a single address to which a bridge listens when it receives STP information. Each bridge on the network sends STP packets to the group address. Every bridge on the network receives STP packets that were sent to the group address, regardless of which bridge sent the packets.

Although 802.1d specifies what the group address should be, older products from different vendors may respond to different group addresses. If STP does not seem to be working in a mixed-vendor environment, other vendors' products may have different group addresses. In that case, you need to set the STP group address.



1 To set the STP group address, from the top level of the Administration Console, enter:

```
bridge stpGroupAddress
```

2 Enter the group address at the prompt.

For IBM Spanning Tree Protocol, the group address is C0:00:00:00:01:00

Administering Trunks

You can configure the system to aggregate multiple network links into a single *trunk*. This trunking feature lets you create high-speed point-to-point or multipoint connections without changing or replacing existing cabling.

The system treats trunked ports in much the same way as individual ports. Also, all higher-level network functions — including Spanning Tree algorithms, VLANs, and SNMP management— treat a trunk as indistinguishable from any other network port.

One important difference, though, is that the system automatically distributes traffic across *all* ports associated with a trunk. If any of the trunk's ports go down or up, the system automatically redistributes traffic across the new set of operational ports.

When a trunk is created for ports that are already part of a VLAN, those ports are removed from the VLAN. If the ports are part of the default VLAN, they remain as part of the default VLAN. You must modify the VLAN and add the new bridge port to the appropriate VLAN. Please note that this is does not apply to the default VLAN.

Valid Trunk Configurations

The system supports four trunks, each built from up to six ports. All channels in a trunk must connect:

- Correctly configured ports
- Identical types of ports (with no two ports *on a trunk* connected to the same network)
- Identical types of network nodes (switches, bridges, or end-stations)

Trunks can connect just two network nodes (a *point-to-point* trunk) or up to eight nodes (a *multipoint* trunk).

Point-to-Point Trunk

Figure 8-1 shows a *point-to-poin*t trunk. This example combines six 100-Mbps Fast Ethernet ports into a 600-Mbps trunk. The system automatically allocates traffic among the six ports on the trunk, and reallocates traffic if any of these ports go down or up.

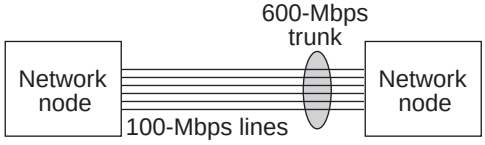


Figure 8-1 A Point-to-Point Trunk Combining Six Fast-Ethernet Ports

This configuration is useful for building temporary or permanent high-speed pipelines between two fixed nodes or locations.

Multipoint Trunk

Figure 8-2 illustrates a *multipoint* trunk configuration connecting three network nodes across three independent Fast Ethernet LAN segments.

Three Fast Ethernet ports on each node are combined into a single 300-Mbps trunk. Each port within a trunk connects to a different LAN segment. The nodes automatically allocate traffic within their trunks and reallocate traffic if any ports go down or up.

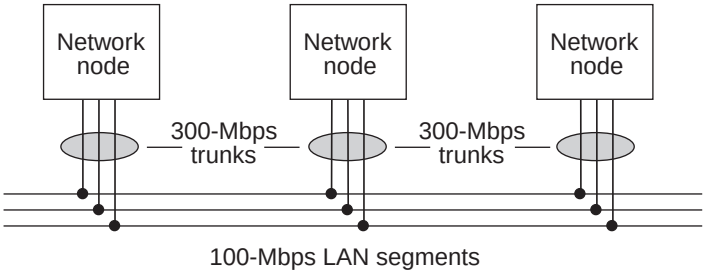


Figure 8-2 A Multipoint Trunk Connecting Three Network Nodes

This configuration offers several immediate network improvements without requiring any changes to existing LANs or to the system hardware:

- Higher aggregate bandwidth to and from each network node
- Transmission of 100-, 200-, and 300-Mbps data streams between all nodes
- Automatic traffic allocation within each trunk
- Guaranteed correct sequencing of packets within a single data stream
- Improved network reliability, from redundant parallel LAN segments

Trunk Port Numbering

When you combine ports on a trunk, the system treats the entire trunk as a single bridge port, identified by a single bridge port number in bridge statistics. For example, the following two figures show how bridge port numbers change when ports 2, 3, and 4 are trunked.

Figure 8-3 shows how the ports are numbered in Ethernet and bridge statistics before trunking.

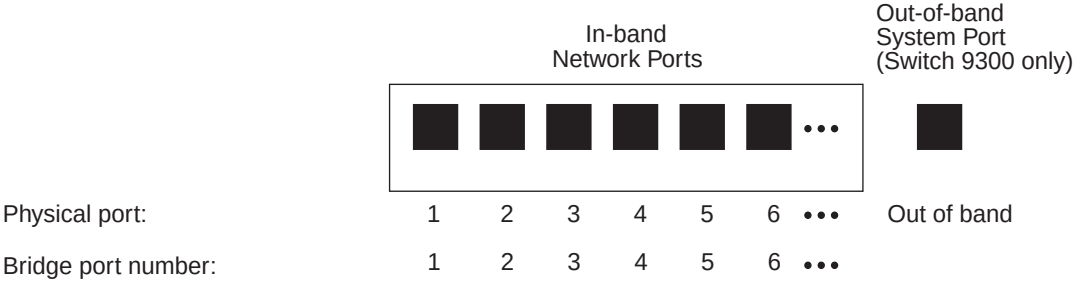


Figure 8-3 Bridge Port Numbering Before Trunking

Figure 8-4 shows how the ports are numbered in Ethernet and bridge statistics after trunking. The entire trunk becomes bridge port number 2 in bridge port statistics. And bridge ports 5 and 6 in Figure 8-3 become ports 3 and 4 after trunking.

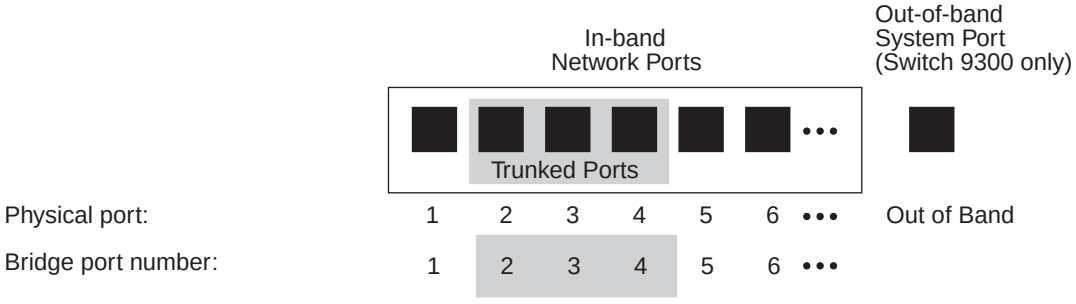


Figure 8-4 Bridge Port Numbering After Trunking

TCMP Protocol

The system uses a proprietary Trunk Control Message Protocol (TCMP) to perform the following functions:

- Automatically detect and correct trunks that violate trunk configuration rules
- Ensure orderly activation and deactivation of ports on a trunk

The system runs a separate TCMP agent for each trunk. If TCMP detects an invalid configuration (see "Valid Trunk Configurations" on page 8-9) the protocol automatically restricts the trunk to the largest subset of ports that is a valid configuration.

Enabling TCMP is optional, but recommended. If TCMP is disabled, the network will still function, but without automatic trunk validation and reconfiguration. By default, TCMP is enabled.

TCMP Operations

Each TCMP agent:

- Periodically transmits a TCMP *helloMessage* through every trunk port
- Continuously listens for *helloMessages* from other ports on the system
- Builds a list of ports that TCMP has detected
- Uses this list to activate or deactivate ports to maintain valid trunk configurations

TCMP uses three trunk port states to control port activation and deactivation:

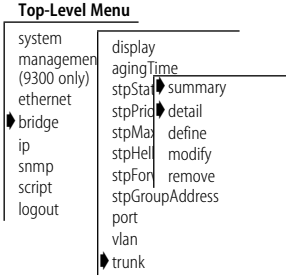
- **notInUse** — A trunk port in this state has not been *selected* to participate in the trunk.
- **selected** — TCMP has selected the port to participate in the trunk, but the trunk port has not yet become active.
- **inUse** — A trunk port that is fully active on the trunk.

Displaying Trunking Information

You can display summary or detail information about trunks on your system.

From the top level of the Administration Console, enter:

```
bridge trunk summary
```



or

```
bridge trunk detail
```

Sample bridge trunk summary display:

```
Trunk summary

Macs 1-12=Gigabit Ethernet

Index  Name              State      TCMP       Port  Macs
    1  GAtoCA            up         enabled       6  6-8
```

Sample bridge trunk detail display:

```
Trunk detail

Macs 1-12=Gigabit Ethernet

Index  Name              State      TCMP       Port  Macs
    1  GAtoCA            up         enabled       6  6-8

Index  Node trunk id            Mac type          Present macs  Missing macs
    1  00-80-3e-46-43-54-00-00  Gigabit Ethernet             3             0

Index    Mac  Trunk state  Tcmp state
    1      6  up           inUse
    1      7  up           inUse
    1      8  up           inUse

Index    Mac       rxFrames       rxHellos       txFrames       txHellos
    1      6          35874          35874          36074          36074
    1      7          35838          35838          36039          36039
    1      8          35837          35837          36039          36039

Index    Mac   rxBadVersion      rxBadType  rxSameTrunkId     rxOverflow
    1      6              0              0              0              0
    1      7              0              0              0              0
    1      8              0              0              0              0

Index         Selected node trunk id list
    1         00-80-3e-46-0c-e3-00-00

Index    Mac  Node trunk id list
    1      6  00-80-3e-46-0c-e3-00-00
    1      7  00-80-3e-46-0c-e3-00-00
    1      8  00-80-3e-46-0c-e3-00-00
```

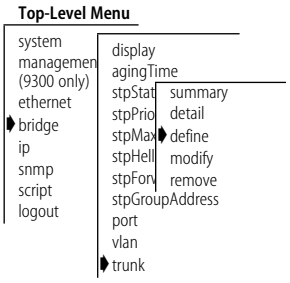
Each item in the trunk displays is described in Table 8-2.

Table 8-2 Trunk Attributes

Parameter	Description
Index	The identifier that the system assigned to the trunk.
Missing ports	The number of ports that are configured for the trunk, but missing because an interface card is inaccessible.
Name	The name assigned to the trunk.
Node trunk id	The TCMP identifier assigned to the trunk.
Node trunk id list	The `Node trunk ids` that each port has detected on the trunk.
Port	The bridge port number assigned to the trunk.
Present ports	Number of ports participating in the trunk.
rxBadType	Number of TCMP messages received that contain a bad *type* field.
rxBadVersion	Number of TCMP messages received that contain a bad TCMP *version number*.
rxFrames	Number of TCMP messages received on each port.
rxHellos	Number of TCMP *helloMessages* received on each port.
rxOverflow	Number of times that TCMP has detected a TCMP trunk configuration that exceeds the eight node maximum.
rxSameTrunkId	Number of times that TCMP has received a *helloMessage* containing the TCMP agent's own `Node trunk id` (an illegal configuration)
Selected node trunk id list	The `Node trunk ids` selected for use on the trunk.
State	Indicates whether the trunk is `up` or `down`.
TCMP	Indicates whether TCMP is `enabled` or `disabled` for the trunk.
Tcmp state	The TCMP state for each port in the trunk: ■ `notInUse` — Not selected for use in the trunk. ■ `selected` — Selected for use in the trunk, but not yet active in the trunk. ■ `inUse` — Active in the trunk.
Trunk state	State (`up` or `down`) of each port link in the trunk.
txFrames	Number of TCMP messages transmitted on each port.
txHellos	Number of TCMP *helloMessages* transmitted on each port.

Defining a Trunk

When you define a trunk, you specify several characteristics associated with the trunk.



1 To define a trunk, from the top level of the Administration Console, enter:

`bridge trunk define`

Enter the information associated with the trunk. Press Return or Enter to accept the existing value in brackets.

2 Enter the name of the trunk.

The name can have up to 16 characters.

3 Specify whether TCMP is *enabled* or *disabled.*

The system default is *enabled.*

4 Select the port type.

5 Specify the ports that constitute the trunk.

The maximum number of ports per trunk is eight.

6 Select the trunk mode.

You can choose 10 Mbps, 100 Mbps, or 1000Mbps running in half-duplex or full-duplex mode. All ports in the trunk will be set to this type.

7 At the system prompt, enter **y** (yes) to reboot the system and implement the trunk or **n** (no) to return to the previous menu.

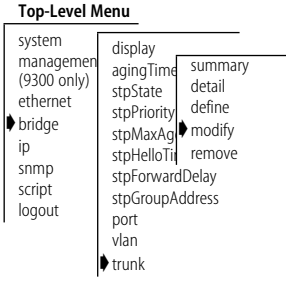
Entering **n** (no) cancels the trunk definition.

Sample Switch 3900:

```
Enter trunk name: CampusLink
Enter TCMP state (disabled,enabled) [enabled]:
Select mac type [Fast Ethernet,Gigabit Ethernet]: fast
Select up to 6 mac(s) (1-18|all): 1-6
Enter mac mode {10half,10full,100half,100full}: 100full
The system must be rebooted to complete trunk configuration
Are you sure you want to reboot the system? (n,y) [y]:
```

Modifying a Trunk

You can modify a trunk's characteristics. If you add or remove a port, the system requests a reboot to implement the change. All other changes occur immediately, without interrupting trunk operations.



1 To modify a trunk, from the top level of the Administration Console, enter:

```
bridge trunk modify
```

Enter the information associated with the trunk. Press Return or Enter to accept the existing value in brackets.

2 Enter the name of the trunk.

The name can have up to 16 characters.

3 Specify whether TCMP is *enabled* or *disabled.*

The system default is *enabled.*

4 Select the port type.

5 Specify the ports that constitute the trunk.

The maximum number of ports per trunk is eight.

CAUTION: *If you add or remove a port, the system requests a reboot to implement the change.*

6 Select the trunk mode.

You can choose 10 Mbps, 100 Mbps, or 1000 Mbps running in half-duplex or full-duplex mode. All ports in the trunk will be set to this type.

7 If you added or removed a port in step 5, the system displays a reboot prompt.

Enter **y** (yes) to reboot the system and implement the trunk changes or **n** (no) to return to the previous menu.

Entering **n** (no) cancels the trunk changes.

Example:

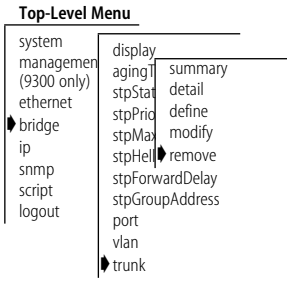
```
Enter trunk index [1]:
Enter trunk name [CampusLink]:
Enter TCMP state (disabled,enabled) [disabled]:
Select mac type [Fast Ethernet,Gigabit Ethernet]:
Select up to 6 mac(s) (1-18|all) [1-4]: 1-3
Enter mac mode {10half,10full,100half,100full} [100full]:
The system must be rebooted to complete trunk configuration
Are you sure you want to reboot the system? (n,y) [y]:
```

Removing a Trunk

Use this command to remove a previously defined trunk. This command removes only one trunk at a time.

From the top level of the Administration Console, enter:

```
bridge trunk remove
```



1 Enter the trunk index number.

2 At the system prompt, enter **y** (yes) to reboot the system and remove the trunk or **n** (no) to return to the previous menu.

Entering **n** (no) cancels the trunk removal.

Example:

```
Enter trunk index [1]:
The system must be rebooted to complete trunk configuration
Are you sure you want to reboot the system? (n,y) [y]:
```

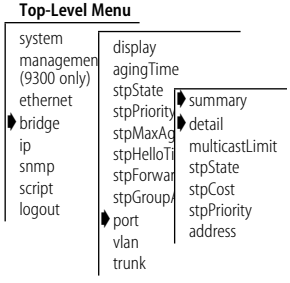
9 ADMINISTERING BRIDGE PORTS

This chapter describes how to view and manage bridge port information in the SuperStack II® Switch 3900 and Switch 9300 systems using the following tasks:

- Displaying Bridge Port Information
- Setting the Multicast Limit
- Administering STP Bridge Port Parameters
- Administering Port Addresses

Displaying Bridge Port Information

Bridge port information includes the STP configurations for the bridge port. You can display this information in either summary or detail format.



1. To display bridge information, from the top level of the Administration Console, enter:

   `bridge port summary`

   or

   `bridge port detail`

2. Select the port type: **`Ethernet`**
3. Enter one or more port numbers or **`all`** to view port parameters for all ports on the bridge.

Sample bridge port summary display:

```
       port             rxFrames          rxDiscards             txFrames
Ethernet  1              1328325                 273                    4
Ethernet  2                    0                   0                    1
Ethernet  3                    0                   0                    1
Ethernet  4                    0                   0                    1
Ethernet  5                    0                   0                    1
Ethernet  6               107699                   0              1436341

       port                                    portId       fwdTransitions
Ethernet  1                                    0x8001                    1
Ethernet  2                                    0x8002                    0
Ethernet  3                                    0x8003                    0
Ethernet  4                                    0x8004                    0
Ethernet  5                                    0x8005                    0
Ethernet  6                                    0x8006                    1

       port                 stp           linkState              state
Ethernet  1             enabled                  up         forwarding
Ethernet  2             enabled                down           disabled
Ethernet  3             enabled                down           disabled
Ethernet  4             enabled                down           disabled
Ethernet  5             enabled                down           disabled
Ethernet  6             enabled                  up         forwarding
```

Sample bridge port detail display:

```
       port             rxFrames                              rxSameSegDiscs
Ethernet  1              1330089                                           2
Ethernet  2                    0                                           0
Ethernet  3                    0                                           0
Ethernet  4                    0                                           0
Ethernet  5                    0                                           0
Ethernet  6               107783                                           0

       port         rxErrorDiscs     rxMcastLimitType         rxMcastLimit
Ethernet  1                    0          McastBcast                    0
Ethernet  2                    0          McastBcast                    0
Ethernet  3                    0          McastBcast                    0
Ethernet  4                    0          McastBcast                    0
Ethernet  5                    0          McastBcast                    0
Ethernet  6                    0          McastBcast                    0

       port      rxMcastExcDiscs       rxMcastExceeds      rxSecurityDiscs
Ethernet  1                    0                    0                    0
Ethernet  2                    0                    0                    0
Ethernet  3                    0                    0                    0
Ethernet  4                    0                    0                    0
Ethernet  5                    0                    0                    0
Ethernet  6                    0                    0                    0

       port         rxOtherDiscs      rxForwardUcasts        rxFloodUcasts
Ethernet  1                    0                    0               348322
Ethernet  2                    0                    0                    0
Ethernet  3                    0                    0                    0
Ethernet  4                    0                    0                    0
Ethernet  5                    0                    0                    0
Ethernet  6                    0                    0               107789

       port      rxForwardMcasts             txFrames               portId
Ethernet  1               981560                    4               0x8001
Ethernet  2                    0                    1               0x8002
Ethernet  3                    0                    1               0x8003
Ethernet  4                    0                    1               0x8004
Ethernet  5                    0                    1               0x8005
Ethernet  6                    0              1438266               0x8006

       port       fwdTransitions                  stp            linkState
Ethernet  1                    1              enabled                   up
Ethernet  2                    0              enabled                 down
Ethernet  3                    0              enabled                 down
Ethernet  4                    0              enabled                 down
Ethernet  5                    0              enabled                 down
Ethernet  6                    1              enabled                   up

       port              state             priority             pathCost
Ethernet  1          forwarding                 0x80                    1
Ethernet  2            disabled                 0x80                    1
Ethernet  3            disabled                 0x80                    1
Ethernet  4            disabled                 0x80                    1
Ethernet  5            disabled                 0x80                    1
Ethernet  6          forwarding                 0x80                    1

       port       designatedCost       designatedPort       designatedRoot
Ethernet  1                   30               0x8015    8000 00803e028e16
Ethernet  2                    0                  0x0    0000 000000000000
Ethernet  3                    0                  0x0    0000 000000000000
Ethernet  4                    0                  0x0    0000 000000000000
Ethernet  5                    0                  0x0    0000 000000000000
Ethernet  6                   31               0x8006    8000 00803e028e16

       port     designatedBridge                                       macs
Ethernet  1    8000 00803e291801                                         1
Ethernet  2    0000 000000000000                                         2
Ethernet  3    0000 000000000000                                         3
Ethernet  4    0000 000000000000                                         4
Ethernet  5    0000 000000000000                                         5
Ethernet  6    8000 00803e46434f                                       6-8
```

Table 9-1 describes the type of information that the system provides for the bridge port.

Table 9-1 Bridge Port Attributes

Parameter	Description
fwdTransitions	Number of times that the port has entered forwarding state. This value is useful for checking the stability of a bridged topology. The more transitions in and out of the forwarding state, the more unstable is the topology.
portId	Identification of the port, which includes the port priority and the port number (for example: 8002)
priority	First factor that determines if a port is to be the designated port when more than one bridge port is attached to the same LAN. If all ports in a bridge have the same priority, then the port number is used as the determining factor.
rxErrorDiscs	Number of frames that were discarded by this port because of internal bridge system errors (such as hardware and software address table discrepancies)
rxFloodUcasts	Number of unicast frames received on this port that were flooded to one or more ports
rxForwardMcasts	Number of multicast frames received on this bridge port that were forwarded to another bridge port
rxForwardUcasts	Number of unicast frames received on this bridge port that were forwarded to another bridge port
rxFrames	Number of frames that were received by this port from its segment. A frame received on the interface that corresponds to this port is only counted by this object if the frame is for a protocol being processed by the local bridging function, including bridge management frames.
rxMcastExcDiscs	Number of multicast frames that were discarded when rxMcastLimit was exceeded
rxMcastExceeds	Amount of time that rxMcastLimit has been exceeded
rxMcastLimit	Configurable parameter that limits the rate of multicast frames that are forwarded on a bridge port
rxSameSegDiscs	Number of frames that were discarded by this port because the destination address is known on the same network segment as the source address (that is, the frame does not need to be bridged)
rxSecurityDiscs	Number of frames that were discarded by this port because they contained source addresses that were statically configured on another bridge port (that is, a statically configured station, which is not allowed to move, appears to have moved)

(continued)

Table 9-1 Bridge Port Attributes (continued)

Parameter	Description
state	Spanning Tree state *(blocking, listening, learning, forwarding, disabled)* in which the port is currently operating: *Blocking*: The bridge continues to run the Spanning Tree algorithm on the port, but the bridge does not receive data packets from the port, learn locations of station addresses from it, or forward packets onto it. *Listening*: The bridge continues running the Spanning Tree algorithm and transmitting configuration messages on the port, but it discards data packets received on the port and does not transmit data packets forwarded to the port. *Learning*: Similar to listening, but the bridge receives data packets on the port to learn the location of some of the stations located on the port. *Forwarding*: The bridge receives packets on the port and forwards or does not forward them depending on address comparisons with the bridge's source address list. *Disabled*: The port has been disabled by management.
stp	Whether the Spanning Tree Protocol is *enabled* or *disabled* for the port
txFrames	Number of frames that were transmitted by this port to its segment. A frame transmitted on the interface corresponding to this port is counted by this object only if the frame is for a protocol that is being processed by the local bridging function, including bridge management frames.

Frame processing and bridge port statistics

Any frame that is received on a physical interface and not explicitly directed to the system is delivered to the corresponding bridge port. The system either forwards the frame to another bridge port or discards it. The system can discard a frame for the following reasons:

- The destination station is on the same segment as the source station.
- The receive bridge port is blocked.
- There is some problem with the frame.

Figure 9-1 shows the order in which discard decisions are made.

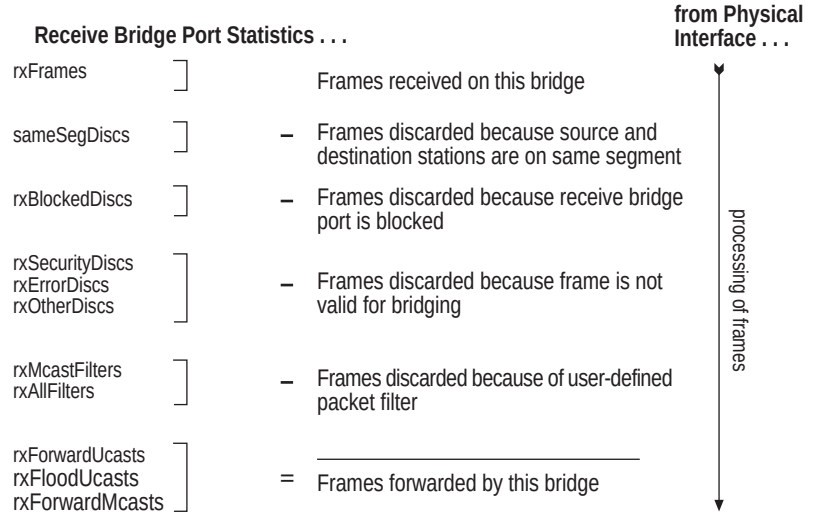


Figure 9-1 How Frame Processing Affects Receive Bridge Port Statistics

A frame that is forwarded to a bridge port is transmitted onto a physical interface unless it is discarded for one of the following reasons:

- The transmit bridge port is blocked.
- The frame is too large for the corresponding physical interface.

Figure 9-2 shows the order in which the discard decisions are made.

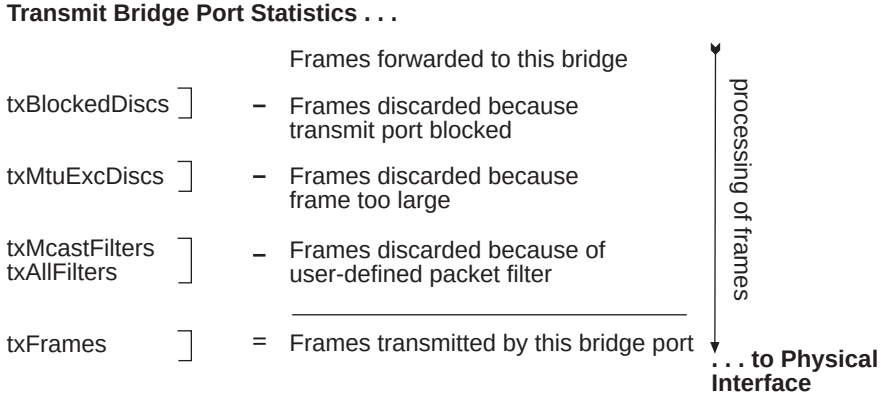
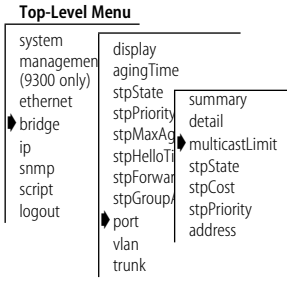


Figure 9-2 How Frame Processing Affects Transmit Bridge Port Statistics

Setting the Multicast Limit

You can assign a multicast packet firewall threshold to a bridge port on the system. This threshold limits the forwarding rate of multicast traffic that originates on the Fast Ethernet segment connected to the port.

Default The default is zero *(0),* which indicates that no threshold exists.



1 To set the multicast limit, from the top level of the Administration Console, enter:

```
bridge port multicastLimit
```

2 Enter the port type: **`Ethernet`**

3 Enter one or more port numbers or **`all`** to set the threshold for ports on the bridge.

The system prompts you for a new value for each port you specified.

4 Enter the new multicast threshold value for each port.

Example:

```
Fast Ethernet port 3 - Enter new value [0]: 400
Fast Ethernet port 4 - Enter new value [0]: 400
```

Administering STP Bridge Port Parameters

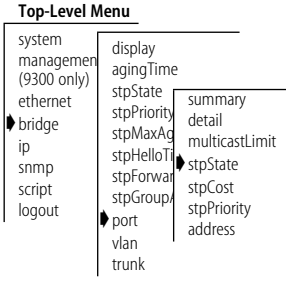
You can enable or disable the Spanning Tree Protocol for one or more ports on the system. This setting affects the operation of a port only if the Spanning Tree Protocol is enabled. You can also set the following STP port parameters: path cost and priority.

Enabling and Disabling STP on a Port

You can enable and disable the Spanning Tree Protocol for any port on the system. When STP is disabled for a port but enabled for the entire bridge, a port does not forward frames or participate in the Spanning Tree algorithm. When STP is disabled for a port as well as for the entire bridge, the port will continues to forward frames.

If a port is configured as removed, it is not considered in the Spanning Tree even if STP is enabled for the bridge. In this state, the port will forward frames as long as the link is up.

Default By default, the Spanning Tree state value on a port is enabled.



1. To enable or disable STP on a port, from the top level of the Administration Console, enter:

   `bridge port stpState`

2. Enter the port type: **`Ethernet`**
3. Enter one or more port numbers or **`all`** to enable or disable ports for the Spanning Tree Protocol.

   The system prompts you for a new value for each port that you specified.
4. Enter **`enabled`**, **`disabled`**, or **`removed`** at the prompts.

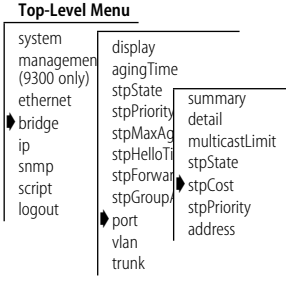
   Example of setting values for more than one port:

```
Fast Ethernet port 4 - Enter new value (disabled,enabled,removed)
[enabled]: disabled
Fast Ethernet port 5 - Enter new value (disabled,enabled,removed)
[enabled]: disabled
```

Setting the Port Path Cost

You can set the path cost for a bridge port. The path cost is the cost that the algorithm adds to the root cost field in a configuration message that is received on this port. This value is used to determine the path cost to the root through this port. You can set this value individually on each port.

Path cost value A larger path cost value makes the LAN that is reached through the port more likely to be low in the Spanning Tree topology. The lower the LAN is in the topology, the less through traffic it carries. For this reason, you may want to assign a large path cost to a LAN that has a lower bandwidth or one on which you want to minimize traffic.



1. To configure the path cost, from the top level of the Administration Console, enter:

   `bridge port stpCost`

2. Enter the port type: **`Ethernet`**
3. Enter one or more port numbers or **`all`** to configure the path cost for ports on each bridge.
4. Enter the path cost for the ports that you specified.

   Example of setting values for more than one port:

```
Fast Ethernet port 3 - Enter new value [100]:  200
Fast Ethernet port 4 - Enter new value [100]: 200
```

If your configuration is successful, the previous menu appears on the screen.

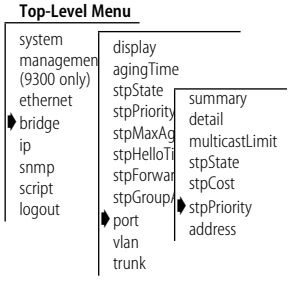
If the configuration is not successful, the system notifies you that your changes failed, and you can try to reenter your changes.

Setting the Port Priority

The STP port priority influences the choice of port when the bridge has two ports connected to the same LAN, creating a loop. The port with the lowest port priority is used by the Spanning Tree Protocol.

Port priority value

Port priority is a 1-octet value.



1. To configure port priority, from the top level of the Administration Console, enter:

   `bridge port stpPriority`

2. Enter the port type: **`Ethernet`**
3. Enter one or more port numbers or **`all`** to configure the port priority for ports on each bridge.
4. Enter the port priority for the ports that you specified.

   Example of setting values for more than one port:

   ```
   Fast Ethernet port 3 - Enter new value [0x80]: 1
   Fast Ethernet port 4 - Enter new value [0x80]: 500
   ```

   If your configuration is successful, the previous menu appears on the screen.

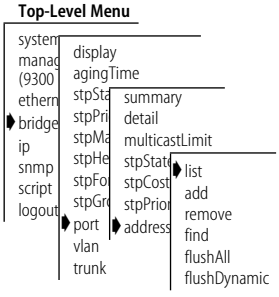
   If the configuration is not successful, the system notifies you that your changes failed, and you can try to reenter your changes.

Administering Port Addresses

You can administer the MAC addresses of stations that are connected to Ethernet ports on the system.

Listing Addresses

You can display the MAC addresses that are currently associated with the selected ports. The display includes each address type (static or dynamic), assigned port, and age.



1 To list currently defined MAC addresses, from the top level of the Administration Console, enter:

`bridge port address list`

2 Enter the port type: **`Fast Ethernet`**

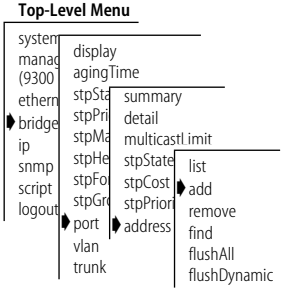
3 Enter one or more port numbers or **`all`** to display the MAC addresses for the ports that you selected.

Sample bridge port address list:

```
Addresses for Ethernet port 2:
Cononical address       Type
08-00-20-1d-67-e2       Dynamic
00-80-3e-02-68-00       Dynamic
00-20-af-29-7b-74       Dynamic
08-00-02-05-91-c1       Dynamic
00-80-3e-02-6d-00       Static
00-80-3e-08-5f-00       Dynamic
00-80-3e-00-3d-00       Dynamic
```

Adding New Addresses

When you assign new MAC addresses to the selected ports, the system adds them as statically configured addresses. A statically configured address is never aged out of the address table and can never be learned on a different Fast Ethernet port.



1 To add (statically configure) a MAC address, from the top level of the Administration Console, enter:

`bridge port address add`

2 Enter the port numbers.

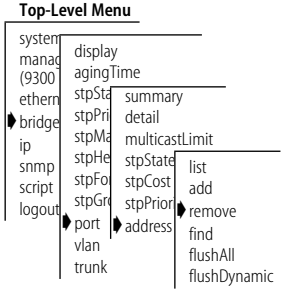
The system prompts you for one or more addresses to add.

3 Type each MAC address, pressing Enter after each entry.

4 Enter **`q`** to return to the previous menu when you finish entering addresses.

Removing Addresses

You can remove individual MAC addresses from selected ports.



1 To remove a MAC address, from the top level of the Administration Console, enter:

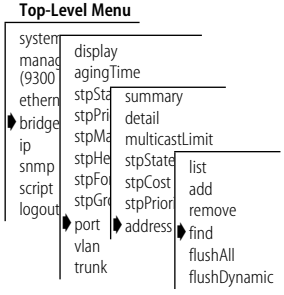
```
bridge port address remove
```

2 Enter the addresses to remove, pressing Enter after each entry.

3 Enter **q** to return to the previous menu when you have entered all of the addresses that you want to remove.

Finding a Port Address

You can determine the MAC address associated with a port.



1 From the top level of the Administration Console, enter:

```
bridge port address find
```

2 Enter the MAC address that you want to find.

The system displays the address and the port that is associated with it.

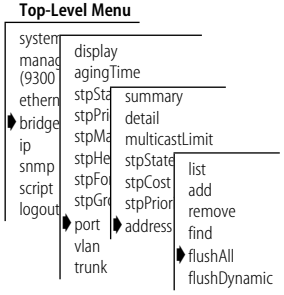
Example bridge port address find:

```
Enter address: 08-00-20-79-10-f8
Address found on Ethernet port 1:
   Canonical address Type
   08-00-20-79-10-f8 Static
```

Flushing All Addresses

You can flush all static and dynamic MAC addresses from the ports you select.

- **Static MAC addresses** — Address that you specified using the *add* menu option
- **Dynamic MAC addresses** — Addresses that the bridge learned automatically



1 To flush all addresses, from the top level of the Administration Console, enter:

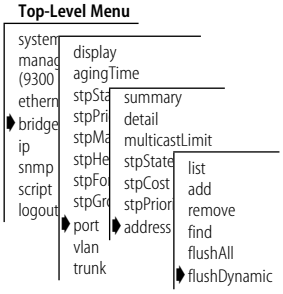
```
bridge port address flushAll
```

2 Enter one or more port numbers or **all**

The system flushes all addresses from the ports that you specified.

Flushing Dynamic Addresses

You can flush all dynamic (automatically learned) addresses from the ports that you select.



1. To flush dynamic addresses, from the top level of the Administration Console, enter:

   `bridge port address flushDynamic`

2. Enter one or more port numbers or **`all`**

   The system flushes the addresses from the address table.

10 Administering Virtual LANs (VLANs)

This chapter describes how to manage and display information about VLANs using the following tasks:

- Displaying VLAN Information
- Defining VLAN Information for a Bridge
- Modifying VLAN Information
- Removing a VLAN

To administer VLANs, you must be familiar with the following terms:

- A *VLAN* is a logical definition of a network workgroup and is roughly equivalent to a Layer 2 broadcast domain. VLANs can be seen as analogous to a group of end-stations, perhaps on multiple LAN segments, that are not constrained by their physical location and can communicate as if they were on a common LAN.
- A *VLAN interface* is your bridge's point of attachment to a given VLAN. A VLAN interface exists entirely within a single bridge; you control the configuration of the VLAN interfaces on your bridge. You can think of a VLAN and a VLAN interface as analogous to an IP subnet and an IP interface. Your system supports three types of VLAN interfaces: port-based, protocol-based, and network-based.

A VLAN interface can be defined to contain multiple bridge ports.

- *Tagging* refers to a method used to include implicit or explicit VLAN membership information within each frame. *Implicit tagging* refers to a protocol; *explicit tagging* refers to an IEEE 802.1Q tag. Each port within a VLAN interface can operate with one of the following explicit tagging types:
  - **None** — With this form of tagging, frames are sent using the same format on non-VLAN links.
  - **802.1Q tagging** — With this form of tagging, frames are encapsulated and tagged as specified in the IEEE 802.1Q standard. This form of tagging encodes the IEEE 802.1Q header and the VLAN ID inside the frames.

A bridge port may be shared by multiple VLAN interfaces as long as there is some form of tagging that provides a distinguishing characteristic for the shared port.

- The *VLAN mode* specifies a VLAN as all open or all closed.
  - A VLAN mode of *all open* (the default VLAN mode for all VLANs) permits data to be forwarded between VLANs without causing a security violation. For example, data can be received on VLAN 2 with a destination of VLAN 3 can be forwarded to there. This mode implies that the system uses a single bridge address table (the default configuration).
  - A VLAN mode of *all closed* means that data cannot be forwarded between VLANs. This implies that there is an address table for each VLAN.

Your system is initially configured to support a default VLAN interface that contains all of the bridge ports, with unspecified protocol information and no tagging.

Displaying VLAN Information

You can display a summary of VLAN information or a detailed report:

- In a summary report, the system displays the protocols and ports that are assigned to each VLAN.
- The detailed VLAN report includes the summary information plus additional utilization statistics.

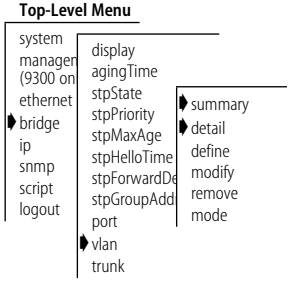
From the top level of the Administration Console, enter:

`bridge vlan summary`

or

`bridge vlan detail`

The system displays the VLAN information in the format that you specified.



Sample VLAN summary display:

```
VLAN summary

VLAN Mode: allOpen

Ports 1-10=Ethernet

Index   VID  Type    Origin  Name                    Ports
    1     1  open    static  Default                 1-10
```

Sample VLAN detail display:

```
VLAN detail

VLAN Mode: allOpen

Ports 1-10=Ethernet

Index   VID  Type    Origin  Name                    Ports
    1     1  open    static  Default                 1-10

Index  Port  Tag Type
    1     1  none
    1     2  none
    1     3  none
    1     4  none
    1     5  none
    1     6  none
    1     7  none
    1     8  none
    1     9  none
    1    10  none
```

Table 10-1 describes these attributes.

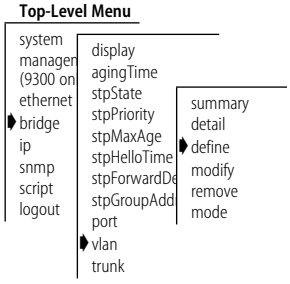
Table 10-1 VLAN Attributes

Field	Description
Index	System-assigned index that identifies a VLAN
VID	Unique, user-defined (4-byte) integer used by global management operations. The VID is used as the 802.1Q tag if tagging is enabled.
Ports	The numbers of the ports that are assigned to the VLAN
Name	16-byte character string that identifies the members of the VLAN
Tag type	802.1Q or none
Mode	The VLAN mode type; all open or all closed

Defining VLAN Information for a Bridge

Follow these steps to create a VLAN definition for a bridge. Press Enter to accept the default value that appears in brackets [ ].

You can define a maximum of 127 VLANs on a single bridge. By default, all ports are defined to be part of the default VLAN.



1 From the top level of the Administration Console, enter:

```
bridge vlan define
```

2 Enter the VLAN identification (VID) number: *1* through *4095.*

3 Enter the VLAN name, which can include up to 32 ASCII characters and spaces. If you use spaces, put quotation marks around the VLAN name.

4 Enter one or more port numbers or **all** to assign all ports to the VLAN.

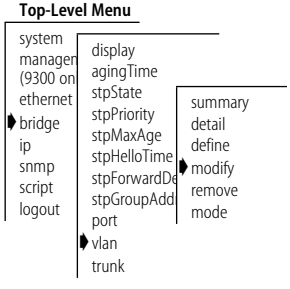
5 Configure the per port tagging,

Example of defining a Switch 3900 VLAN:

```
menu option (bridge/vlan): define
Enter VID (1-4095): 2
Enter VLAN name []:Marketing
Enter ports (1-39|all):1
Configure per port tagging (n,y) [y]:
Enter port 1 tag type (none, 802.1Q):none
```

Modifying VLAN Information

Follow these steps to modify VLAN information for a bridge.



1 From the top level of the Administration Console, enter:

```
bridge vlan modify
```

The system prompts you to reenter the information that defines the VLAN. Press [Return] to accept any value that appears in brackets [ ].

2 Enter the VLAN identification (VID) number: 1 through 4095.

3 Enter the VLAN name. The VLAN name can include up to 32 ASCII characters, including spaces. If you include spaces, surround the VLAN name with quotes.

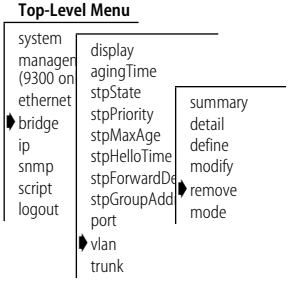
4 Enter one or more port numbers or **all** to assign all ports to the VLAN.

5 Modify per port tagging.

Sample modification of a Switch 3900 VLAN:

```
menu option (bridge/vlan): modify
Enter VID (1-4095): 2
Enter VLAN name []:Marketing
Enter ports (1-39|all):1
Configure per port tagging (n,y) [y]:
Enter port 1 tag type (none, 802.1Q):
```

Removing a VLAN



Follow these steps to remove a VLAN definition:

1 From the top level of the Administration Console, enter:

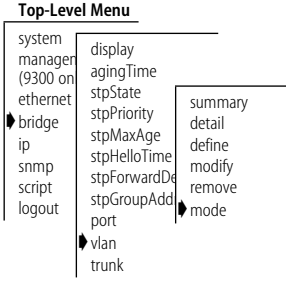
`bridge vlan remove`

2 Enter the indexes for the VLANs that you want to remove.

Example:

```
Select menu option (bridge/vlan): remove
Select VLAN interface index(es) (1-2|all): 1
```

Setting the VLAN Mode

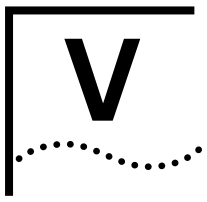


You can select the VLAN mode as all open or all closed. The default is all open.

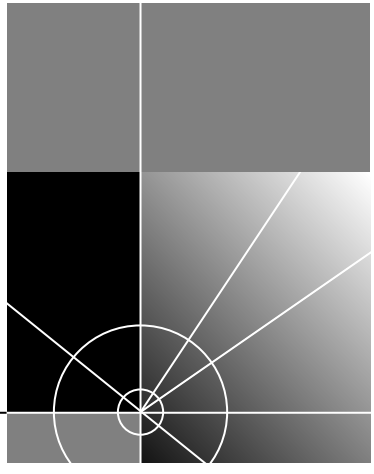
1 From the top level of the Administration Console, enter:

`bridge vlan mode`

2 Enter the VLAN mode (**`allOpen`** or **`allClosed`**).



IP MANAGEMENT



11 ADMINISTERING IP

This chapter describes how to configure Internet Protocol (IP) interfaces on the SuperStack® II Switch 3900 and Switch 9300 using the following tasks:

- Administering IP Interfaces
- Administering Routes
- Administering the ARP Cache
- Administering RIP
- Administering the Domain Name Server Client
- Using the Ping Function
- Administering traceRoute
- Displaying IP Statistics

Administering IP Interfaces

An interface defines the relationship between an IP Virtual LAN (VLAN) and the subnets in the IP network. Every IP VLAN interface has one IP VLAN associated with it. The system has one interface defined for each subnet directly connected to it.

You must first define a VLAN, as described in Chapter 10, before you define an associated IP VLAN interface.

Interface Characteristics

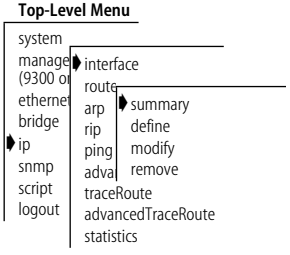
Each IP routing interface has the following characteristics associated with it:

- **IP address** — Choose this address from the range of addresses assigned to your organization by the central agency. This address is specific to your network.

- **Subnet mask** — A 32-bit number that uses the same format and representation as IP addresses. The subnet mask determines which bits in the IP address are interpreted as the network number, the subnet number, and the host number. Each IP address bit corresponding to a 1 in the subnet mask is in the network/subnet part of the address. Each IP address bit corresponding to a 0 is in the host part of the IP address.
- **VLAN index** — This is the number of the IP VLAN associated with the IP interface. The VLAN index indicates which bridge ports are associated with the IP interface. When the menu prompts you for this option, it displays a list of available VLAN indexes and the ports associated with them.

Displaying Interfaces

You can display summary information about all IP interfaces configured on the system. The detail display contains all the summary information as well as information about the advertisement address.



To display IP interface information, from the top level of the Administration Console, enter:

```
ip interface summary
```

Sample IP interface summary display:

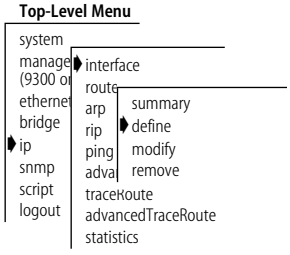
```
IP routing is disabled

Index  Type        IP address       Subnet mask      State  Port index
    1  System      158.101.154.102  255.255.255.0    Up             1
```

Defining an Interface

When you define an IP interface, you specify several characteristics associated with that interface, as well as the VLAN associated with it. (When you manage your system in-band, you need to define an interface with these characteristics.)

The default values that the system provides for some interface characteristics are appropriate for most networks.

You must first define a VLAN, as described in Chapter 10, before you define an associated IP VLAN interface.



1 To define an IP interface, from the top level of the Administration Console, enter:

`ip interface define`

The system prompts you for the interface's parameters. To use the value in the brackets, press [Return] at the prompt.

2 Enter the IP address of the interface.

3 Enter the subnet mask of the interface.

4 Enter the interface type (vlan or system).

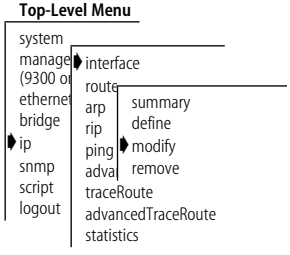
5 Enter the VLAN interface index.

Sample results from **`ip interface define`**:

```
Enter IP address: 158.101.1.1
Enter subnet mask [255.255.0.0]: 255.255.255.0
Enter interface type (vlan, system [vlan]:vlan
Enter VLAN interface index [2]:2
```

Modifying an IP Interface

You can change the configuration of an interface that you have already defined.



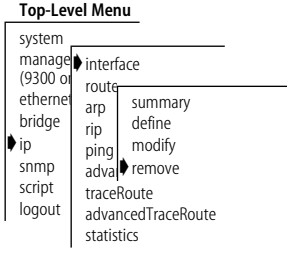
1 To modify an IP interface, from the top level of the Administration Console, enter:

`ip interface modify`

2 Modify the existing interface parameters by entering a new value at the prompt.

Removing an Interface

You can remove an interface if you are no longer using it to route on the ports associated with the interface.



1 To remove an IP interface definition, from the top level of the Administration Console, enter:

`ip interface remove`

2 Enter the index number of the interface you want to remove.

Administering Routes

The system maintains a table of routes to other IP networks, subnetworks, and hosts. You can make static entries in this table using the Administration Console, or you can configure the system to use RIP to automatically gather routing information .

Each routing table entry contains the following information:

- **Destination IP address and subnet mask** — These elements define the address of the destination network, subnetwork, or host. A route matches an IP address if the bits in the IP address that correspond to the bits set in the route subnet mask match the route destination address. If the system finds more than one routing table entry that matches an address, it uses the most specific route, which is the route with the most bits set in its subnet mask. For example, the route to a subnetwork within a destination network is more specific than the route to the destination network.
- **Routing metric** — This metric specifies the number of networks or subnetworks through which a packet must pass to reach its destination. The system includes the metric in its RIP updates to allow other routers to compare routing information received from different sources.
- **Gateway IP address** — This address tells the router how to forward packets whose destination addresses match the route's IP address and subnet mask. The system forwards such packets to the indicated gateway.
- **Status** — For each interface, the route provides the status information in Table 11-1.

Table 11-1 Interface Status Information

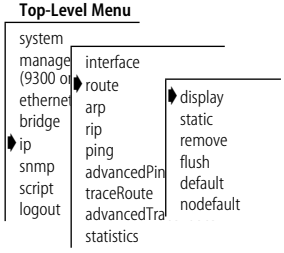
Field	Description
Direct	Route goes to a directly connected network
Static	Route was statically configured
Learned	Route was learned using indicated protocol
Timing out	Route was learned but is partially timed out
Timed out	route has timed out and is no longer valid

In addition to the routes to specific destinations, the routing table can contain an additional entry called the *default route*. The system uses the default route to forward packets that do not match any other routing

table entry. You may want to use the default route in place of routes to numerous destinations that all have the same gateway IP address.

Displaying the Routing Table

You can display the system's routing table to determine which routes are configured and whether the routes are operational.

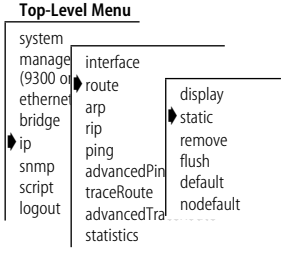


To display the contents of the routing table, from the top level of the Administration Console, enter:

```
ip route display
```

Defining a Static Route

Before you can define static routes, you must define at least one IP interface. (See the section "Defining an Interface" on page 11-2 for details.) Static routes remain in the table until you remove them or the corresponding interface. Static routes take precedence over dynamically learned routes to the same destination.



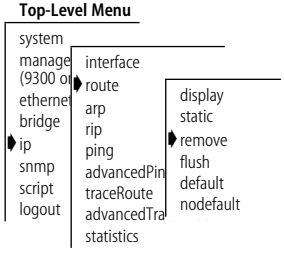
1. To define a static route, from the top level of the Administration Console, enter:

   ```
   ip route static
   ```

   The Administration Console prompts you for the route's parameters. To use the value in brackets, press Return or Enter at the prompt.
2. Enter the destination IP address of the route.
3. Enter the subnet mask of the route.
4. Enter the gateway IP address of the route.

Removing a Route

You can remove an existing route.



1. To remove a route, from the top level of the Administration Console, enter:

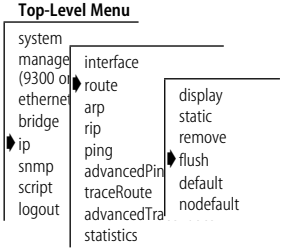
   ```
   ip route remove
   ```
2. Enter the destination IP address of the route.
3. Enter the subnet mask of the route.

   The system immediately deletes the route from the routing table.

Flushing All Learned Routes

Flushing deletes all learned routes from the routing table.

To flush all learned routes, from the top level of the Administration Console, enter:



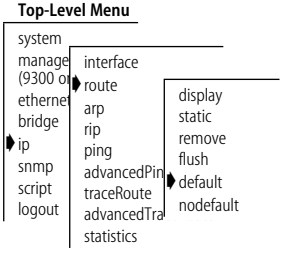

```
ip route flush
```

The system deletes all learned routes from the routing table immediately.

Setting the Default Route

If you define a default route, the system uses it to forward packets that do not match any other routing table entry. The system can learn a default route using RIP, or you can configure a default route statically.

If the routing table does not contain a default route, either statically configured or learned using RIP, then the system cannot forward a packet that does not match any other routing table entry. If this occurs, the system drops the packet.



To statically configure the default route, from the top level of the Administration Console, enter:

```
ip route default
```

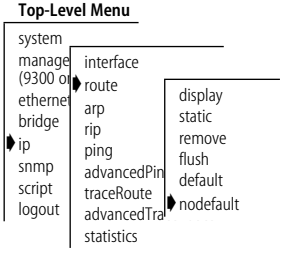
Enter the gateway IP address.

The system adds the default route to the routing table immediately.

Removing the Default Route

This command removes a default route from the routing table.

To remove a default route from the routing table, from the top level of the Administration Console, enter:




```
ip route nodefault
```

The system removes the default route from the routing table immediately.

Administering the ARP Cache

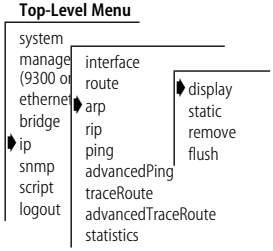
The system uses the Address Resolution Protocol (ARP) to find the MAC addresses that correspond to the IP addresses of hosts and other routers on the same subnetworks. Each device that participates in routing maintains an ARP cache, that is, a table of known IP addresses and their corresponding MAC addresses.

Displaying the ARP Cache

You can display the contents of the ARP cache for each interface on the system.

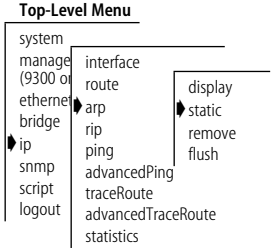
To display the contents of the ARP cache, from the top level of the Administration Console, enter:

```
ip arp display
```



Defining a Static ARP Cache Entry

You can define a static ARP cache entry on the system.



1. To define a static ARP cache entry, from the top level of the Administration Console, enter:

   ```
   ip arp static
   ```

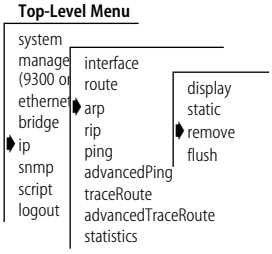
2. Enter the IP address of the ARP cache entry.
3. Enter the MAC address of the ARP cache entry.

   Example:

   ```
   Select interface index {1-2} 2
   Enter IP address: 158.101.12.12
   Enter MAC address: 00-80-3e-02-8e-70
   ```

Removing an ARP Cache Entry

You can remove an entry from the ARP cache if the MAC address has changed.



1 To remove an ARP cache entry, from the top level of the Administration Console, enter:

```
ip arp remove
```

2 Enter the IP address of the entry that you want to remove.

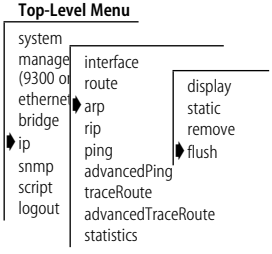
The system immediately removes the address from the ARP cache. If necessary, the system subsequently uses ARP to find the new MAC address that corresponds to that IP address.

Flushing the ARP Cache

You can delete all entries from the ARP cache if the MAC address has changed.

To remove all entries form the ARP cache, from the to level of the Administration Console, enter:

```
ip arp flush
```



The system immediately removes the entries from the ARP cache.

Administering RIP

The Routing Information Protocol (RIP) is one of the IP Interior Gateway Protocols (IGPs). The system uses RIP to dynamically configure its routing tables.

RIP operates in terms of active and passive devices. The *active devices*, usually routers, broadcast their RIP messages to all devices in a network or subnetwork; they update their own routing tables when they receive an RIP message from another device. The *passive devices*, usually hosts, listen for RIP messages and update their routing tables; they do not send RIP messages.

An active router sends a RIP message every 30 seconds. This message contains both the IP address and a metric (the distance to the destination from that router) for each destination. In RIP, each router through which a packet must travel to reach a destination equals one *hop*.

Setting the RIP Mode

You can select one of two RIP modes on the system:

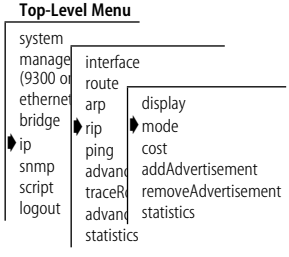
- **Off** — The system ignores all incoming RIP packets and does not generate any RIP packets of its own.
- **Passive** — The system processes all incoming RIP packets and responds to explicit requests for routing information, but it does *not* broadcast periodic or triggered RIP updates.

Default The default RIP mode is *passive*.

Follow these steps to set the RIP mode on the system.

1 From the top level of the Administration Console, enter:

```
ip rip mode
```

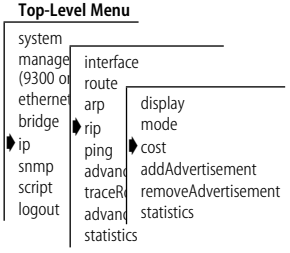


2 Enter the RIP mode: **`off`** or **`passive`**. To use the value in brackets, press Return or Enter at the prompt.

Setting the Cost

You can set the RIP cost option.

Default The default cost value is *1,* which is appropriate for most networks.



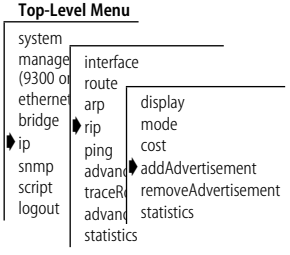
1. To set the cost value, from the top level of the Administration Console, enter:

   `ip rip cost`

2. Select the interface from the available interfaces (for example, *1-4* or *all*).
3. Enter the cost value for the specified interfaces. The range is from *1* through *15.*

Adding an Advertisement Address

You can add an advertisement address to the IP RIP interface.



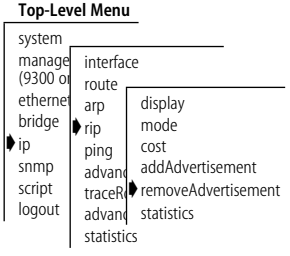
1. To add an advertisement address, from the top level of the Administration Console, enter:

   `ip rip addAdvertisement`

2. Enter the IP interface index number.
3. Enter an advertisement address. You can specify up to 32 advertisement addresses in separate iterations.

Removing an Advertisement Address

You can remove an advertisement address from the advertisement address list that is associated with the interface.

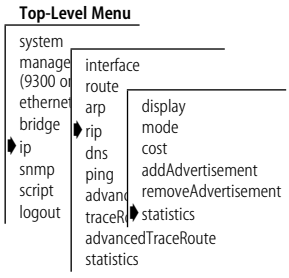


1. To remove an advertisement address, from the top level of the Administration Console, enter:

   `ip rip removeAdvertisement`

2. Enter the IP interface index number and the advertisement address that you want to remove.

Displaying RIP Statistics



You can display RIP statistics.

To display RIP statistics, from the top level of the Administration Console, enter:

```
ip rip statistics
```

Sample RIP statistics:

```
RIP general statistics

          routeChanges                queries
                    73                      0
```

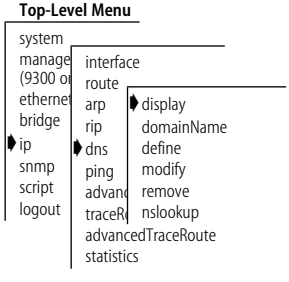
Administering the Domain Name Server Client

The system Domain Name Server (DNS) client provides DNS lookup functionality to the system's IP ping and traceRoute features. This functionality allows you to specify a hostname rather than an IP address when you perform various operations (for example, when you use ping or traceRoute to contact an IP station).

The DNS commands allow you specify one or more name servers that are associated with a domain name. Each name server maintains a list of IP addresses and their associated host names. When you use ping or traceRoute with a hostname, the DNS client attempts to locate the name on the name servers that you specify. When the DNS client locates the name, it resolves it to the associated IP address.

See UNIX NFS documentation for information about how to create and maintain lists of domain names and IP addresses on the name servers.

Displaying the DNS Configuration



You can display the current domain name and the name servers associated with it.

From the top level of the Administration Console, enter:

```
ip dns display
```

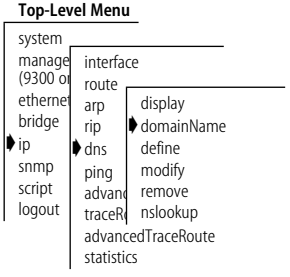
The system displays the current DNS configuration.

Example:

```
Domain Name - synnet
Name Server - 158.101.112.7
              158.101.112.2
              158.101.112.9
```

Modifying the DNS Domain Name

You can change the name of a currently defined domain.



1. To modify a domain name, from the top level of the Administration Console, enter:

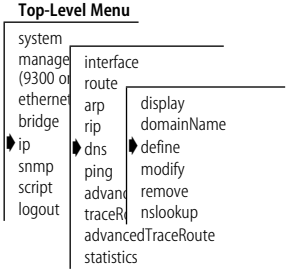
   `ip dns domainName`

2. Enter the new domain name, or specify **`?`** to get information about specifying a domain name. The system displays the current domain name in brackets.

   You can specify a domain name with up to 79 characters. Use quotes around any string with embedded spaces. Use `""` to enter an empty string.

Defining a New Name Server IP Address

You can define a new name server IP address associated with the current domain name.



1. To define a new name server IP address, from the top level of the Administration Console, enter:

   `ip dns define`

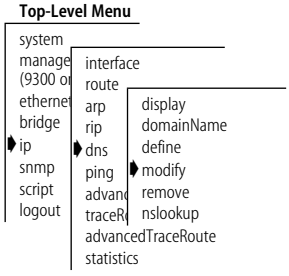
2. Enter the new name server IP address at the prompt. When the system accepts the new IP address, it displays a message similar to the following:

   ```
   Server's IP address xxxxx is added to the DNS database
   ```

   The system assigns an index number to the new IP address. Use this index number to modify or remove this IP address.

Modifying a Name Server IP Address

You can modify a currently defined name server IP address.



1 To modify a name server IP address, from the top level of the Administration Console, enter:

```
ip dns modify
```

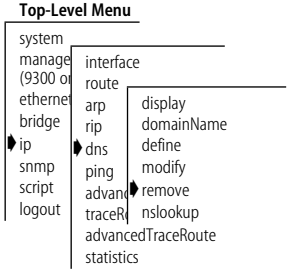
The system displays the list of name server addresses and the index number that is associated with each.

2 Enter the server index number of the IP address that you want to modify, or specify **?** to get a list of the selectable server indexes.

3 Enter the new IP address.

Removing a Name Server IP Address

You can remove a previously defined Name Server IP address.



1 To remove a name server IP address, from the top level of the Administration Console, enter:

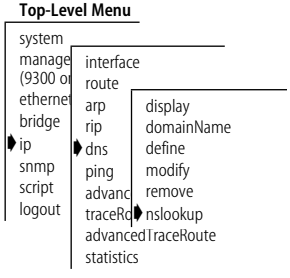
```
ip dns remove
```

The system displays the list of Name Server IP addresses and the index number associated with each address.

2 Enter the index number of the IP address that you want to remove, or specify **?** to get a list of the selectable server indexes.

Querying Name Servers

You can resolve an IP address to a host name or a host name to an IP address on a name server. You enter either the host name or the IP address: the DNS client displays the pair.



1 To query a name server, from the top level of the Administration Console, enter:

```
ip dns nslookup
```

2 Enter a host name or an IP address at the prompt.

Using the Ping Function

The ping function uses the ICMP echo facility to send ICMP echo request packets to the IP destination you specify. When a router sends an echo request packet to an IP station using ping, the router waits for an ICMP echo reply packet.

The response indicates whether the remote IP is available, unreachable, or not responding. The ping feature is a useful tool for network testing, performance measurement, and management.

The system provides two ping commands to perform the function:

- **`ping`** — Uses the IP address to ping a host with default options
- **`advancedPing`** — Uses the IP address to ping a host with the advanced ping options that you specify

When you specify a hostname with either command, the hostname and its associated IP address must be configured on a network name server. Also, you must add the IP address on the name server to the list of name server addresses that are associated with the network domain name. The section "Administering the Domain Name Server Client" on page 11-11 explains how to do this.

The systems gives one of these responses to a ping:

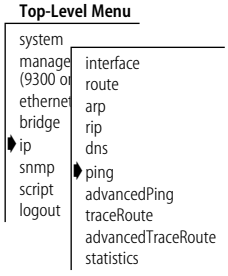
- If the host is reachable, the system displays information about the ICMP reply packets and the response time to the ping. The amount of information depends on whether the quiet option is enabled or disabled.
- If the host does not respond, the system displays the ICMP packet information and this message: `Host is Not Responding.` (You may see this message if you have not configured your gateway IP address.)
- If the packets cannot reach the host, the system displays the ICMP packet information and this message: `Host is Unreachable.` A host is unreachable when there is no route to that host.

Using the ping Command

The system allows you to ping a destination directly by entering a hostname or IP address with the **`ping`** command.

For example, you can enter **`ip ping 192.156.136.22`**. When you issue the command with the hostname or IP address, the system pings the destination using the default ping options listed in Table 11-2.

To change a ping option, enter **`ip advancedPing`** and then specify the option that you want to change.



1 To ping a host, from the top level of the Administration Console, enter:

`ping`

2 At the prompt, specify the hostname or IP address of the destination that you want to ping.

The following example shows a successful ping with the default options (for example, quiet mode is disabled) and successful hostname resolution through DNS:

```
Select menu option (ip): ping
Enter host name/IP address [0.0.0.0]: 158.101.152.56
Press "Enter" key to interrupt.

PING 158.101.152.56: 64 byte packets
64 bytes from 158.101.152.56:  icmp_seq=0.  time=16. ms
64 bytes from 158.101.152.56:  icmp_seq=1.  time=19. ms
64 bytes from 158.101.152.56:  icmp_seq=2.  time=24. ms

---- 158.101.152.56 PING Statistics ----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 16/20/24
```

Table 11-2 lists the default ping values.

Table 11-2 Default Values for Ping Options

Option	Default
count	3 packets
wait	1 second
packetSize	64 bytes
quiet	disabled
burst	disabled
sourceAddress	determined by the router

Using the advancedPing Command

Use the **`advancedPing`** command to ping a host with one or more of the advanced ping options.

Table 11-3 describes the advanced ping options.

Table 11-3 advancedPing Options

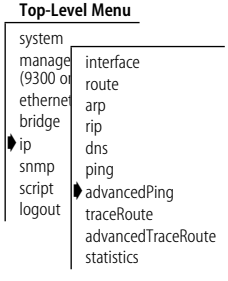
Option	Description
count	The number of ICMP echo request packets that the system sends to ping a host. If the destination host does not respond after being pinged by the number of packets that you specify, the system displays a `Host is Unreachable or Host is not Responding message`. The default count is *3* packets.
wait	The number of seconds that the system waits before it send out successive ICMP echo request packets. You may want to set this option to a high value if network traffic is heavy and you choose not to add to the network traffic with pings in fast succession. The burst option overrides the value set in the wait option. *T*he default is *1* second.
packetSize	The number of bytes in each ICMP echo request packet. The packet size includes both the IP and the ICMP headers. The default is *64* bytes.
quiet	Determines how much packet information the system displays after a ping. When the quiet option is enabled, the system displays summary information about the number of packets the system sent and received, any loss of packets, and the average time it took a packet to travel to and from the host. When the quiet option is disabled, the system displays more detailed status information about each ICMP echo request packet. The default is *disabled.*

(continued)

Table 11-3 advancedPing Options (continued)

Option	Description
burst	When this option is enabled, the system sends out the ICMP echo request packets as rapidly as possible. You can set a high count value (1000 packets, for example) and then observe the run lights on the units: the run lights blink rapidly on routers that are forwarding packets successfully, but remain unlit, or blink slowly, on routers that are not forwarding packets successfully. When this option is enabled, it overrides the value in the wait option, which determines how long the system waits to send out successive ICMP echo packets in a ping. The system displays a period (.) on the screen every time it receives an ICMP echo replay packet. You can use this display to determine how many packets are being dropped during the burst. This output is unique to the burst option and overrides the value set in the quiet option. The default is *disabled*.
sourceAddress	Enables you to force the source address of the ICMP packets to be something other than the IP address of the interface from which the packet originated. This option is available because you can define more than one IP interface on the system. When you enter this command, the system displays a list of currently defined interfaces and their index numbers. Select the index number of the interface you want to use. *The default is determined by the router.*

CAUTION: *The burst option floods the network with ICMP echo packets and can cause network congestion. Do not use the burst option during periods of heavy network traffic. You should use this option only as a diagnostic tool in a network that has many routers to determine if one of the routers is not forwarding packets.*



1. To issue the **`advancedPing`** command with options, from the top level of the Administration Console, enter:

   `ip advancedPing`

2. At the prompt, enter the host name or IP address of the destination host.
3. Enter the number of ICMP request packets that the system will send during a ping. Valid values are *1* through *9999*.

4 Enter the packet size, in bytes. Valid values are *28* through *4096.*

5 Enter the burst mode: **`enabled`** or **`disabled`**.

6 Enter the quiet mode: **`enabled`** or **`disabled`**.

7 Enter the wait value, in seconds. Valid values are *1* through *20*.

8 Configure the ICMP source address.

9 Enter the index number of the interface that you want to use.

10 Press the Enter key to interrupt.

Example:

```
Select menu option (ip): advancedPIng
Enter host name/IP address [158.101.152.56]:
Enter number of ICMP request packets (1-9999) [3]:
Enter packet size (bytes) (28-4096) [64]:
Enter Burst Transmit Ping mode (disabled,enabled) [disabled]:
Enter Quiet mode (disabled,enabled) [disabled]:
Enter time (sec) waits between sending each packet (1-20) [1]:
Configure ICMP sourceAddress? (n,y) [y]:
         Index    Interface address
           0      Best interface (default)
           1      158.101.117.151
Select interface index {0-1|?} [0]: 1
Press “Enter” key to interrupt.

PING 158.101.152.56 from 158.101.117.151: 64 byte packets
64 bytes from 158.101.152.56:  icmp_seq=0.  time=16. ms
64 bytes from 158.101.152.56:  icmp_seq=1.  time=18. ms
64 bytes from 158.101.152.56:  icmp_seq=2.  time=18. ms

---- 158.101.152.56 PING Statistics ----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 16/17/18
```

Administering traceRoute

The traceRoute feature allows you to track the route of an IP packet through the network. The traceRoute information includes all the nodes in the network through which a packet passes to get from its origin to its destination. The traceRoute feature uses the IP time-to-live (TTL) field in UDP probe packets to elicit an ICMP Time Exceeded message from each gateway to a particular host.

The system provides two traceRoute commands to perform the traceRoute function:

- **`traceRoute`** — Uses the IP address to trace a route to a host with the default options
- **`advancedTraceRoute`** — Uses the IP address to trace a route to a host with the advanced traceRoute options that you specify

When you specify a hostname with the command, the hostname and its associated IP address must be configured on a network name server. Also, you must add the IP address on the name server to the list of name server addresses that are associated with the network domain name. The section "Administering the Domain Name Server Client" on page 11-11 explains how.

To track the route of an IP packet, the traceRoute feature launches UDP probe packets with a small TTL value and then listens for an ICMP Time Exceeded reply from a gateway. Probes start with a small TTL of 1 and increase the value by one until one of the following events occurs:

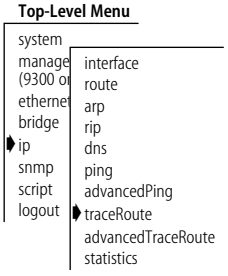
- The system receives a Port Unreachable message, indicating that the packet reached the host.
- The probe exceeds the maximum number of hops. The default is *30* hops.

At each TTL setting, the system launches three UDP probe packets, and the traceRoute display shows a line with the TTL value, the address of the gateway, and the round trip time of each probe. If a probe answers from different gateways, the traceRoute feature prints the address of each responding system. If no response occurs in the 3 second time-out interval, traceRoute displays an asterisk * for that probe.

Issuing the traceRoute Command

The system allows you trace a route by entering a hostname or IP address with a single traceRoute command. For example, you can enter **`ip traceRoute 192.156.136.22`**. Issuing the command with the hostname or IP address causes the system to track the route to the destination using the default options. (See Table 11-4 for a list of the default traceRoute options.)

To change any ping options, use the format **`ip advancedTraceRoute`** and then specify the options that you want to change at the prompts.



1 To issue traceRoute directly, from the top level of the Administration Console; enter:

`traceRoute`

2 At the prompt, specify the hostname or IP address of the destination.

The following example shows a successful traceRoute with the default options:

```
Select menu option (ip): traceRoute
Enter host name/IP address [0.0.0.0]: 158.101.152.56
Press "Enter" key to interrupt.

Traceroute to 158.101.152.56: 30 hops max, 28 bytes packet

  1  158.101.117.254  8 ms
```

The system begins the trace and then displays the IP address and hostname (if available) of the gateways and routers through which the UDP probe packets pass on the way to the destination.

Table 11-4 lists the default traceRoute values.

Table 11-4 TraceRoute Default Values

Option	Default
time-to-live **ttl**	30 hops
base port number **port**	33434
number of probes **probeCount**	3
maximum time to wait	3 seconds
bytes per UDP packet **packetSize**	28 bytes

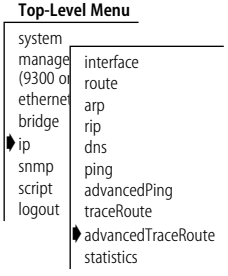
Using the advancedTraceRoute Command

The advancedTraceRoute command provides more controls and flexibility over the traceRoute application.

Table 11-5 describes the advanced traceRoute options.

Table 11-5 advancedTraceRoute Options

Option	Description
ttl	Determines the maximum number of hops that the system can use in outgoing probe packets. The default is *30* hops.
destination port number	The *port number* is the destination (or base) UDP port number that the system uses in probe packets. Set the destination UDP port number to be very high to ensure that an application at the destination is not using that port. Valid port numbers are larger than 30,000, making use of the destination UDP port very unlikely. The default base port number is *33434*.
probe count	The maximum number of probes that the systems sends out at each ttl level. The default value is *3*.
wait	The number of seconds that the system waits before it send out successive ICMP echo request packets. You may want to set this option to a high value if network traffic is heavy and you choose not to add to the network traffic with requests in fast succession. The burst option overrides the value set in the wait option. The default is *1* second.
packetSize	The number of bytes in each ICMP echo request packet. The packet size includes both the IP and the ICMP headers. The default is *64* bytes.
sourceAddress	Enables you to force the source address of the ICMP packets to be something other than the IP address of the interface from which the packet originated. This option is available because you can define more than one IP interface on the system. When you enter this command, the system displays a list of currently defined interfaces and their index numbers. Select the index number of the interface you want to use. *The default is determined by the router.*
numeric mode	When you enable this option, the system prints hop addresses numerically rather than symbolically. The default value is *disabled*.



1 To issue the advancedTraceRoute command with options, from the top-level of the Administration Console; enter:

   `ip advancedTraceRoute`

2 At the prompt, enter the host name or the IP address of the destination.

3 Enter the maximum ttl value.

4 Enter the destination port number.

5 Enter the maximum number of probes that the system sends at each ttl level. Valid probe count values are *1* through *10*.

6 Enter the time, in seconds, for the wait response.

7 Enter the packet size value.

8 Enter the index number of the source address that you want to specify.

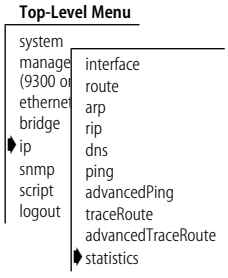
9 Enter the numeric mode: **`enabled`** or **`disabled.`**

   Example:

```
Select menu option (ip): advancedTraceRoute
Enter host name/IP address [158.101.152.56]:
Enter maximum Time-to-Live (ttl) (1-255) [30]:
Enter Destination Port number (30000-65535) [33434]:
Enter the number of probes to be sent at each ttl level (1-10)
[3]:
Enter time (sec) to wait for a response (1-10) [3]:
Enter the packet size (bytes) (28-4096) [28]:
Configure TRACEROUTE sourceAddress? (n,y) [y]:
         Index    Interface address
           0      Best interface (default)
           1      158.101.117.151
Select interface index {0-1|?} [0]: 1
Enter Numeric mode (disabled,enabled) [disabled]:
Press "Enter" key to interrupt.

Traceroute to 158.101.152.56 from 158.101.117.151: 30 hops max, 28
bytes packet

  1  158.101.117.254  11 ms
```

Displaying IP Statistics

You can display different types of IP statistics: general statistics and those specific to UDP or ICMP.



1 From the top level of the Administration Console, enter:

```
ip statistics
```

2 Enter the type of statistics that you want to display: **`ip`**, **`udp`**, **`icmp`**, or **`all`**

Sample displays for IP, UDP, and ICMP statistics:

```
IP general statistics

          inReceived          inHdrErrors         inAddrErrors
                   0                    0                    0

       forwDatagrams            unkProtos          inDiscards
                   0                    0                    0

          inDelivers         outRequests         outDiscards
               20162                    0                    0

        outNoRoutes           reasmReqs            reasmOks
                   0                    0                    0

         reasmFails             fragOks           fragFails
                   0                    0                    0

        fragCreates          osReceives         osTransmits
                   0                 5447                    0

         rtDiscards
                   0
```

```
UDP general statistics

         inDatagrams              noPorts             inErrors
               20160                    0                    0

        outDatagrams
                   0
```

```
ICMP general statistics

             messages                inErrors          inDestUnreach
                    0                       0                      0

          inTimeExcds            inParmProbs           inSrcQuenchs
                    0                       0                      0

          inRedirects                inEchos            inEchoReps
                    0                       0                      0

         inTimeStamps     inTimeStampsReps           inAddrMasks
                    0                       0                      0

       inAddrMaskReps                 outMsgs             outErrors
                    0                       0                      0

       outDestUnreach           outTimeExcds          outParmProbs
                    0                       0                      0

        outSrcQuenchs           outRedirects               outEchos
                    0                       0                      0

          outEchoReps           iutTimeStamps     outTimeStampReps
                    0                       0                      0

         outAddrMasks       outAddrMaskReps
                    0                       0
```

Table 11-6 describes the IP, UDP, and ICMP general IP statistics.

Table 11-6 IP Statistics

Field	Description
forwDatagrams	Number of datagrams that the IP station tried to forward
fragCreates	The number of IP datagram fragments generated as a result of fragmentation on this system
fragFails	The number of IP datagrams discarded because they needed to be fragmented but could not be (for example, their Don'tFragment bit was set)
fragOks	The number of IP datagrams that successfully fragmented
inAddrErrors	Number of datagrams that the IP station discarded because of an error in the source or destination IP address
inDelivers	Number of datagrams that the IP station delivered to local IP client protocols
inDiscards	Number of packet receive discards
inHdrErrors	Number of datagrams that the IP station discarded because the IP header contained errors

(continued)

Table 11-6 IP Statistics (continued)

Field	Description
inReceived	Total number of IP datagrams received, including those with errors
osReceives	Number of packets received that are destined to higher-level protocols such as telnet, DNS, TFTP, and FTP
osTransmits	Number of packets sent through the router by higher-level protocols such as telnet, DNS, TFTP, and FTP
outDiscards	Number of packet transmit discards
outNoRoutes	Number of datagrams that the IP station discarded because there was no route to the destination
outRequests	Number of datagrams that local IP client protocols passed to IP for transmission
reasmFails	The number of packet reassembly failures
reasmReqs	The number of packet reassembly requests
reasmOks	The number of successful packet reassemblies
rtDiscards	Number of packets discarded due to system resource errors
unkProtos	Number of packets whose protocol is unknown

Table 11-7 describes the UDP statistics.

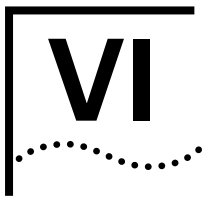
Table 11-7 UDP Statistics

Field	Description
inDatagrams	Number of UDP packets received and addressed to the router or broadcast address
inErrors	Number of received UDP or ICMP packets that contain header errors
noPorts	Number of UDP packets received but addressed to an unsupported UDP port
outDatagrams	Number of UDP packets sent by the router

Table 11-8 describes the ICMP statistics.

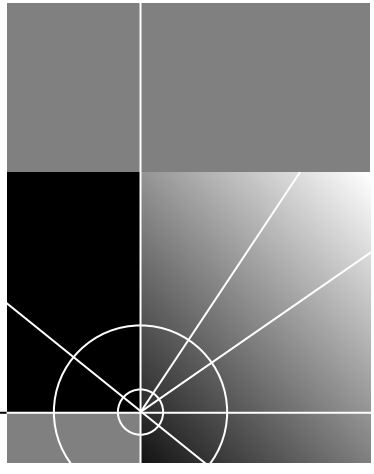
Table 11-8 ICMP Statistics

Field	Description
inAddrMaskReps	Number of ICMP address mask reply frames received
inAddrMasks	Number of ICMP address mask request packets received
inDestUnreach	Number of ICMP destination unreachable packets received
inEchoReps	Number of ICMP echo reply packets received
inEchos	Number of ICMP echo request packets received
inParmProbs	Number of ICMP parameter problem frames received
inRedirects	Number of ICMP redirect packets received
inSrcQuenchs	Number of ICMP source quench packets received
inTimeExcds	Number of ICMP time exceeded packets received
inTimeStamps	Number of ICMP time stamp request packets received
inTimeStampsReps	Number of ICMP time stamp reply packets received
messages	Number of ICMP packets received
outAddrMaskReps	Number of ICMP address mask reply packets sent
outAddrMasks	Number of ICMP address mask request packets sent
outDestUnreach	Number of ICMP destination unreachable packets sent
outEchoReps	Number of ICMP echo reply packets sent
outEchos	Number of ICMP echo request packets sent
outErrors	Number of ICMP packets sent that were dropped due to system resource errors
outMsgs	Number of ICMP packets sent
outParmProbs	Number of ICMP parameter problem packets sent
outRedirects	Number of ICMP redirect packets sent
outSrcQuenchs	Number of ICMP source quench packets sent
outTimeExcds	Number of ICMP time exceeded packets sent
outTimeStampReps	Number of ICMP time stamp reply packets sent
outTimeStamps	Number of ICMP time stamp request packets sent



APPENDIX

Appendix A Technical Support



TECHNICAL SUPPORT

3Com provides easy access to technical support information through a variety of services. This appendix describes these services.

Information contained in this appendix is correct at time of publication. For the very latest, 3Com recommends that you access the 3Com Corporation World Wide Web site.

Online Technical Services

3Com offers worldwide product support 24 hours a day, 7 days a week, through the following online systems:

- World Wide Web site
- 3Com FTP site
- 3Com Bulletin Board Service (3Com BBS)
- 3ComFacts℠ automated fax service

World Wide Web Site

Access the latest networking information on the 3Com Corporation World Wide Web site by entering the URL into your Internet browser:

`http://www.3com.com/`

This service provides access to online support information such as technical documentation and software library, as well as support options ranging from technical education to maintenance and professional services.

3Com FTP Site

Download drivers, patches, and software across the Internet from the 3Com public FTP site. This service is available 24 hours a day, 7 days a week.

To connect to the 3Com FTP site, enter the following information into your FTP client:

- Hostname: **`ftp.3com.com`** (or **`192.156.136.12`**)
- Username: **`anonymous`**
- Password: **`<your Internet e-mail address>`**

A user name and password are not needed with Web browser software such as Netscape Navigator and Internet Explorer.

3Com Bulletin Board Service

The 3Com BBS contains patches, software, and drivers for 3Com products. This service is available through analog modem or digital modem (ISDN) 24 hours a day, 7 days a week.

Access by Analog Modem

To reach the service by modem, set your modem to 8 data bits, no parity, and 1 stop bit. Call the telephone number nearest you:

Country	Data Rate	Telephone Number
Australia	Up to 14,400 bps	61 2 9955 2073
Brazil	Up to 14,400 bps	55 11 5181 9666
France	Up to 14,400 bps	33 1 6986 6954
Germany	Up to 28,800 bps	4989 62732 188
Hong Kong	Up to 14,400 bps	852 2537 5601
Italy	Up to 14,400 bps	39 2 27300680
Japan	Up to 14,400 bps	81 3 3345 7266
Mexico	Up to 28,800 bps	52 5 520 7835
P.R. of China	Up to 14,400 bps	86 10 684 92351
Taiwan, R.O.C.	Up to 14,400 bps	886 2 377 5840
U.K.	Up to 28,800 bps	44 1442 438278
U.S.A.	Up to 28,800 bps	1 408 980 8204

Access by Digital Modem

ISDN users can dial in to the 3Com BBS using a digital modem for fast access up to 56 Kbps. To access the 3Com BBS using ISDN, use the following number:

1 408 654 2703

3ComFacts Automated Fax Service

The 3ComFacts automated fax service provides technical articles, diagrams, and troubleshooting instructions on 3Com products 24 hours a day, 7 days a week.

Call 3ComFacts using your Touch-Tone telephone:

1 408 727 7021

Support from Your Network Supplier

If additional assistance is required, contact your network supplier. Many suppliers are authorized 3Com service partners who are qualified to provide a variety of services, including network planning, installation, hardware maintenance, application training, and support services.

When you contact your network supplier for assistance, have the following information ready:

- Product model name, part number, and serial number
- A list of system hardware and software, including revision levels
- Diagnostic error messages
- Details about recent configuration changes, if applicable

If you are unable to contact your network supplier, see the following section on how to contact 3Com.

Support from 3Com

If you are unable to obtain assistance from the 3Com online technical resources or from your network supplier, 3Com offers technical telephone support services. To find out more about your support options, please call the 3Com technical telephone support phone number at the location nearest you.

When you contact 3Com for assistance, have the following information ready:

- Product model name, part number, and serial number
- A list of system hardware and software, including revision levels
- Diagnostic error messages
- Details about recent configuration changes, if applicable

Here is a list of worldwide technical telephone support numbers:

Country	Telephone Number	Country	Telephone Number
Asia Pacific Rim			
Australia	1 800 678 515	New Zealand	0800 446 398
China		Singapore	800 6161 463
From anywhere in China:	86 21 6350 1590	S. Korea	
From Shanghai:	10 800 3656	From anywhere in S. Korea:	82 2 3455 6455
Hong Kong	800 933 486	From Seoul:	00798 611 2230
India	61 2 9937 5085	Taiwan	0080 611 261
Indonesia	001 800 61 009	Thailand	001 800 611 2000
Japan	0031 61 6439	Pakistan	61 2 9937 5085
Malaysia	1800 801 777	Philippines	1235 61 266 2602
Europe			
From anywhere in Europe, call:	+31 (0)30 6029900 phone +31 (0)30 6029999 fax		
From the following European countries, you may use the toll-free numbers:			
Austria	06 607468	Netherlands	0800 0227788
Belgium	0800 71429	Norway	800 11376
Denmark	800 17309	Poland	0800 3111206
Finland	0800 113153	Portugal	05 05313416
France	0800 917959	South Africa	0800 995014
Germany	0130 821502	Spain	900 983125
Hungary	00800 12813	Sweden	020 795482
Ireland	1 800 553117	Switzerland	0800 55 3072
Israel	177 3103794	U.K.	0800 966197
Italy	1678 79489		
Latin America			
Argentina	541 312 3266	Colombia	571 629 4847
Brazil	55 11 523 2725, ext. 422	Mexico	01 800 849 2273
North America	1 800 NET 3Com (1 800 638 3266)		

Returning Products for Repair

Before you send a product directly to 3Com for repair, you must first obtain a Return Materials Authorization (RMA) number. Products sent to 3Com without RMA numbers will be returned to the sender unopened, at the sender's expense.

To obtain an RMA number, call or fax:

Country	Telephone Number	Fax Number
Asia, Pacific Rim	65 543 6342	65 543 6348
Europe, South Africa, and Middle East	011 44 1442 435860	011 44 1442 435718
From the following European countries, you may call the toll-free numbers; select option 2 and then option 2:		
Austria	06 607468	
Belgium	0800 71429	
Denmark	800 17309	
Finland	0800 113153	
France	0800 917959	
Germany	0130 821502	
Hungary	00800 12813	
Ireland	1 800 553117	
Israel	177 3103794	
Italy	1678 79489	
Netherlands	0800 0227788	
Norway	800 11376	
Poland	0800 3111206	
Portugal	05 05313416	
South Africa	0800 995014	
Spain	900 983125	
Sweden	020 795482	
Switzerland	0800 55 3072	
U.K.	0800 966197	
Latin America	1 408 326 2927	1 408 764 6883
U.S.A. and Canada	1 800 876 3266, option 2	1 408 764 7120

INDEX

L

M

N

O

P

R

S

T

U

V

W

Y